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

OSCAR EDUARDO RAMÍREZ ÁLVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA- SANTANDER
2023

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

AUTOR:
OSCAR EDUARDO RAMÍREZ ÁLVAREZ

M. Sc. JOHN FREDDY QUINTERO TAMAYO
Tutor(a) o Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA- SANTANDER
2023

CONTENIDO

pág.

TABLA ILUSTRACIONES

pág.

GLOSARIO

AMENAZA: Cualquier situación o novedad a la que pueda estar expuesta una organización.

BLUE TEAM: Equipo de seguridad cibernética el cual se encarga de monitorear los sistemas de información en una organización con el fin de identificar ataques externos.

CIBERATAQUE: Equipo de seguridad cibernética el cual se encarga de monitorear los sistemas de información en una organización con el fin de identificar ataques externos.

COPNIA (Consejo Profesional Nacional de Ingeniería): Entidad pública que se encarga de inspeccionar, controlar y vigilar el ejercicio de la ingeniería y sus profesiones afines en Colombia.

DELITO INFORMÁTICO: Se entiende por todo acto delictivo o antijurídico que se lleva a cabo en un entorno digital y/o Internet.

HACKER: Persona o individuo que posee altos conocimientos en informática el cual se dedica a detectar fallos de seguridad en sistemas informáticos y generalmente sacar beneficios de dichos fallos.

RED TEAM: Equipo de seguridad cibernética que tiene como función efectuar ataques controlados a los sistema de información en una entidad u organización, con el fin de conocer e identificar el nivel de preparación en el que se encuentra dicha entidad para así poder hacerle frente a un ataque real.

RIESGO: Es la probabilidad con la que se puede materializar una amenaza, generando como consecuencia la vulnerabilidad o exposición de un sistema.

SEGURIDAD INFORMÁTICA: Es el conjunto de políticas, herramientas, medidas, técnicas y/o acciones que se plantean o se llevan a cabo para poder garantizar la integridad, disponibilidad y confidencialidad de la información.

PENTESTING: Técnicas de penetración que tienen como objetivo realizar ataques a diferentes activos de información en una organización con el fin de encontrar fallos o posibles puntos a vulnerar.

VULNERABILIDAD: Técnicas de penetración que tienen como objetivo realizar ataques a diferentes activos de información en una organización con el fin de encontrar fallos o posibles puntos a vulnerar.

RESUMEN

El resultado esperado con el Seminario Especializado es la construcción de un documento académico producto de un esquema de pruebas para los equipos de seguridad Blue Team y Red Team basado en metodologías de pentesting que permita identificar las vulnerabilidades de ciberseguridad en una organización.

Inicialmente se pretende abordar y/o conocer los aspectos legales que pueden surgir de escenarios específicos y que permitan evaluar la seguridad en una organización, así mismo conocer la legislación que aplica en el territorio nacional o que rige la seguridad informática en nuestro país.

A través del informe a generar se busca describir, demostrar e identificar el empleo de herramientas de gestión y software libre para detectar y contener posible ciberataques por medio del escaneo de vulnerabilidades a las que pueden estar expuestas las organizaciones permitiendo la reducción de brechas de ciberseguridad.

Para llevar a cabo lo anterior descrito es importante generar espacios que cuenten con escenarios de pruebas donde se pueda hacer uso de las diferentes herramientas de gestión que posibiliten el seguimiento de los diversos ataques o en su defecto ocasionar los mismos, con el único propósito de identificar las vulnerabilidades y poder proponer acciones para la reducción de brechas de ciberseguridad en una organización.

ABSTRACT

The expected result of the Specialized Seminar is the construction of an academic document resulting from a testing scheme for the Blue Team and Red Team security teams based on pentesting methodologies that allow the identification of cybersecurity vulnerabilities in an organization.

Initially, it is intended to address and / or know the legal aspects that may arise from specific scenarios and that allow evaluating the security in an organization, as well as knowing the legislation that applies in the national territory or that governs computer security in our country.

Through the report to be generated, the aim is to describe, demonstrate and identify the use of management tools and free software to detect and contain possible cyberattacks through the scanning of vulnerabilities to which organizations may be exposed, allowing the reduction of cybersecurity gaps.

In order to carry out the above described, it is important to generate spaces that have test scenarios where you can use the different management tools that make it possible to monitor the various attacks or, failing that, cause them, with the sole purpose of identifying vulnerabilities and be able to propose actions to reduce cybersecurity gaps in an organization.

INTRODUCCIÓN

El salvaguardar los sistemas de información así como los datos requiere de un conocimiento especializado y también de un entendimiento amplio de estrategias de ataque, tener claro las diversas opciones de tácticas y las herramientas que pueden ser empleadas por los piratas informáticos.

El término “Hacking ético” hace referencia a un grupo de expertos o profesionales que en algunas ocasiones son contratados por las empresas o Entidades con el fin de Hackear su propio sistema para así poder identificar y reparar posibles vulnerabilidades en la red tecnológica de dicha Entidad.

Estos profesionales son expertos cuya especialidad es la de realizar pruebas de penetración o intrusión en los sistemas informáticos, ya sea en Hardware o en Software con el fin de analizar, evaluar, fortalecer y mejorar la seguridad de la red tecnológica de una empresa.

Cada día vienen en aumento los ataques cibernéticos, lo que hace necesario que las organizaciones deban implementar planes y políticas de ciberseguridad que permitan realizar la gestión, administración y mitigación de riesgos en las organizaciones, esto con el fin de poder implementar las medidas necesarias para evitar que un ataque se materialice o que una vulnerabilidad sea explotada.

Las amenazas en una organización pueden ser tanto externas como internas, ya que si no se cuenta con una cultura de seguridad informática dentro de la organización y no hay buenas practicas dentro de la misma, desde adentro de la organización de forma inintencionada se van facilitar situaciones que van a abrir brechas y ocasionar vulnerabilidades en la red de la organización.

Es por lo anterior que el talento humano encargado de la seguridad informática dentro de las organizaciones debe tener muy claro su rol dentro la organización en el momento de un posible ataque informático, así mismo debe estar actualizado y a la vanguardia de las ciberamenazas y contar con herramientas y/o utilidades que permitan dar respuesta oportuna a estos ataques para el impacto que estos puedan generar en la organización no sean irremediable ni devastador.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Realizar un informe técnico de los diferentes escenarios planteados durante el desarrollo del curso, teniendo en cuenta las acciones de los equipos Blue Team y Red Team en la Organización HackerHouse.

1.2 OBJETIVOS ESPECÍFICOS

- Conocer y analizar el marco legal y contexto ético de los equipos Blue Team y Red Team.

- Identificar pasos y procesos Red Team, para la explotación de vulnerabilidades.

- Analizar procesos y aplicar métodos de contención Blue Team.

2. CONCEPTOS EQUIPOS DE SEGURIDAD (CONCEPTO ÉTICO Y LEGAL)

2.1 LEY 1273 DE 2009 Y LEY 1581 DE 2012.

2.1.1 LEY 1273 DE 2009.

La ley 1273 de 2009, basicamente es una ley que regula el tema de los delitos informaticos en el país, dentro de algunos textos leidos, se mencionada que esta ley es una modificación al código penal en Colombia.

A través de esta Ley se busca el proteger tanto los datos como la información, así mismo como la adecuada preservación de los dispositivos y/o medios que hagan uso de las TI. Esta Ley se divide o se separa en dos partes, la primera parte hace referencia a la aplicación de los tres pilares de la seguridad a la información, es decir, la integridad, confidecialidad y disponibilidad de la información, la segunda parte de esta Ley hace referencia a los delitos e infracciones informaticas.

Con el surgimiento de esta Ley, se clasificaron los delitos informaticos en Colombia, y estos se especifican a través de articulos de la siguiente manera:

Art. 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. Alguna que persona que acceda sin autorización previa a un sistema informatico o sobre pase los limites de los permisos otorgados durante su interacción en el mismo, estará expuesto a una sanción en prisión entre 48 y 96 meses y a una sanción economica entre 100 a 1000 SMLMV.

Art. 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMAS INFORMÁTICOS O RED DE TELECOMUNICACIONES. Quien afecte la disponibilidad y/o afecte el funcionamiento a un sistema informatico o a los datos e información que allí se almacenan, estará expuesto a una sanción en prisión entre 48 y 96 meses y a una sanción economica entre 100 a 1000 SMLMV.

Art. 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Quien de forma ilegal, es decir sin previa autorización u orden judicial intercepte comunicación electrómagnetica alguna sin importar el cualquiera de sus fases o actores, estará expuesto a una sanción de prisión de entre 36 y 72 meses.

Art. 269D. DAÑO INFORMÁTICO. Quien afecte la integridad de un sistema informático ajeno, así mismo como la integridad de los datos de terceros, estará expuesto a una sanción en prisión entre 48 y 96 meses y una sanción economica de 100 a 1000 SMLMV.

Art. 269E. USO DE SOFTWARE MALICIOSO. Quien produzca, distribuya o masifique, el que comercialice con algún software dañido o pirata, estará expuesto a una sanción en prisión entre 48 y 96 meses y una sanción economica de 100 a 1000 SMLMV.

Art. 269F. VIOLACIÓN DE DATOS PERSONALES. Quien realice una indebida manipulación de datos personales, sin previa autorización del dueño de estos datos, estará expuesto a una sanción en prisión entre 48 y 96 meses y una sanción economica de 100 a 1000 SMLMV.

Art. 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. Quien diseñe, comercie o promueva paginas WEB falsas que simulen un sitio electrónico confiable con el fin de caputar datos personales o recopilar información bancario de las personas de forma ilegal, estará expuesto a una sanción en prisión entre 48 y 96 meses y una sanción economica de 100 a 1000 SMLMV.

Art. 269I. HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES. Quien de forma ilegal o de manera fraudulenta vulnere la seguridad y/o viole el acceso a un sistema informatico, correo electrónico, red de telecomunicaciones, infaestructura TI, etc, incurrirá en penas sancionatorias.

Art. 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. Quien 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 1500 salarios mínimos legales mensuales vigentes[1].

---

[1] Análisis de la Ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia. [Sitio Web]. Sánchez Castillo, Zulay. [Consultado: 11 de agosto de 2023]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

2.1.2 LEY 1581 DE 2012

La ley 1581 de 2012, es la que rige o regula el tratamiento de los datos personales en Colombia, busca proteger el derecho que tienen todas las personas a conocer, actualizar y rectificar la información o los datos que se hayan recopilado sobre ellas en BD.

Esta Ley aplica tanto a entidades públicas como privadas dentro del país.

Ilustración 1. Ciclo de Vida del Dato

Fuente: Autor

Recolección Datos Personal: Se presenta en el momento en el que el titular del dato personal, entrega dicho dato a la entidad o persona recolectora del mismo.

Esta recolección se puede realizar a través de medios electrónicos, físicos, verbales o mediante conductas inequívocas, esta última corresponde a cuando existe una grabación en un sistema de video vigilancia y se encuentra acompañado de un aviso donde se informa o se notifica de dicha grabación, esto se toma como una autorización.

Almacenamiento: Se presenta cuando el titular del dato personal ha autorizado y entregado su información personal, esta se puede guardar o almacenar, ya sea por medios electrónicos o físicos.

El almacenamiento de la información conlleva la necesidad de proteger la misma de cualquier amenaza que pueda afectar su integridad, confidencialidad y disponibilidad.

Uso del Dato: hace referencia a la forma en cómo se va a utilizar el dato personal que ha sido recolectado y almacenado, el uso debe estar siempre alineado con las finalidades que en su momento le fueron informado al titular del dato personal.

Circulación del Dato: Esta parte del ciclo de vida, hace referencia en donde se está compartiendo dicho dato personal y con quien, ¿ese dato personal tiene transferencia a otras entidades?

Eliminación y/o supresión del dato personal: Esa última parte es importante, ya que se debe garantizar que una vez hecho uso del dato personal, este no pueda ser recuperado o en su defecto según lo que se le haya informado al titular al momento de su autorización y recolección.

2.1.2.1 ROLES

Responsable del tratamiento: Es la Persona o empresas de ámbito natural o jurídico, público o privado, que decide sobre la BD.

Encargado del tratamiento: Quien realiza la manipulación de los datos personales, siguiendo los lineamientos impartidos por el rol anteriormente descrito.

Principios del Tratamiento de DP:

Legalidad: El tratamiento de DP, es una actividad y/o proceso regulado que debe sujetarse a lo establecido en la ley.

Finalidad: El tratamiento de DP, debe tener un objetivo y/o finalidad legítima que esté acorde a la constitución y la ley, dicha finalidad debe ser informada al titular.

Libertad: El desarrollo de la finalidad solo puede ejercerse con consentimiento previo y expreso del titular.

Veracidad: La información suministrada por parte del titular debe ser verás, actualizada, útil, inequívoca, comprobable y clara.

Transparencia: El titular tiene el derecho en cualquier momento a conocer información sobre los datos personales propios que reposen en alguna entidad, esto en cualquier momento y sin restricción alguna.

Acceso y Circulación: Los DP no podrán estar expuestos, solo el personal que cuente con autorización podrá tener acceso a los mismos, de igual forma si circulación no se puede llevar acabo sin que el titular autorice.

Seguridad: La información personal sujeta a tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas a que sean necesarias para otorgar seguridad a los registrados, evitando así su adulteración, pérdida, no disponibilidad, uso o acceso no autorizado o fraudulento.

Confidencialidad: Todas las personas que hagan parte o intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, tanto así cuando ya no tenga nada que ver con esta labor.

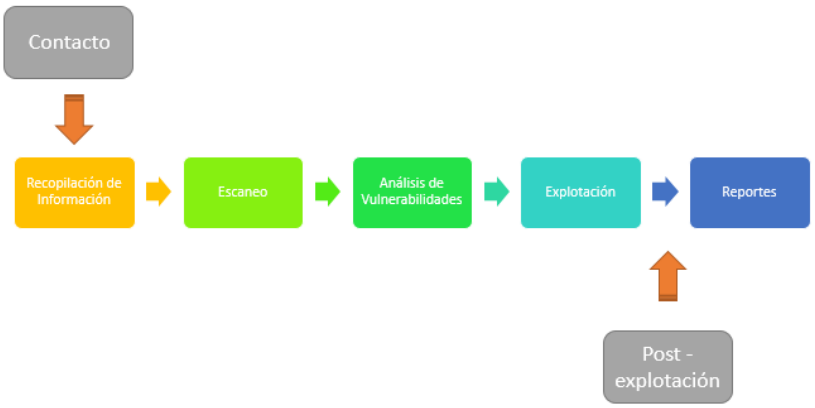
2.1.2.2 TIPOS DE DATOS PERSONALES

- Sensibles
- Privado
- Semiprivado
- Público.

La entidad que en Colombia regula el tratamiento de datos personales, es la SIC (Superintendencia de Industria y Comercio).

2.2 PENTESTING.

Ilustración 2. Fases de Pentesting



Fuente: Autor

Fase I. Interacciones previas o Contacto: En esta fase de comienzo se debe acordar con el cliente las condiciones o aspectos del test de penetración, comprendiendo y dejando claro cuál es o va a ser el objetivo del pentest a realizar, tener claro cuáles son los servicios críticos o más importantes para la empresa y que se vería muy afectado el que hacer de la entidad en caso de un ataque.

En esta fase se debe dejar claro y por escrito diferentes aspectos del test, por ejemplo cual sería el objetivo y la finalidad del proceso a realizar (pentest), los dispositivos o servicios que este va a impactar, así mismo como las IPs a auditar.

Fase II. Recopilación de Información (Footprinting): Esta fase tiene como objetivo obtener toda la información que sea posible sobre la empresa a la cual se le va a realizar el pentesting, esto con el fin de poder hacernos una idea sobre los programas o sistemas en funcionamiento.

Esta etapa es la más importante ya que de ella depende el éxito en el análisis de las vulnerabilidades y la explotación de las mismas, es de tener en cuenta que a mayor información recopilada, mayor será el número de vectores de ataque de los cuales podremos hacer uso.

El proceso de recopilación de información se encuentra divido en dos (2) fases y depende de la forma en que la que se pueda recopilar la información, en el caso que la información recolectada se realiza de manera externa a la organización, esta fase se conoce como External footprinting y si esta información es recogida o conseguida al interior de la empresa, este proceso se conoce como Internal footprinting.

External Footprinting

Existen 2 tipo de de external footprinting, el activo y el pasivo.

Activo: Es el proceso más complejo para obtener información, es necesario realizar el uso de herramientas y técnicas para poder lograrlo, en este tipo se debe interactuar directamente con la infraestructura del objetivo.

Herramientas o Prácticas:

Descubrimiento DNS
Escaneo de Puertos
Descubrimiento SMTP

Pasivo: En este tipo, el contacto no es tan directo con la infraestructura del objetivo, la información o la consulta se realiza por medio de recursos de acceso libre por ejemplo, motores de búsqueda, registros públicos, fotos, etc.

Herramientas o Prácticas:

- Protocolo Whois
- Hacking con buscadores.

Las siguientes con algunas de entre varias herramientas que pueden emplearse para el desarrollo de esta fase:

- Netcraft
- DNSdumpster (Open)
- Shondan
- Maltego
- TheHarvester

Fase III. Escaneo (Modelado de Amenazas): A partir de la información recogida se debe trazar la estrategia de penetración, las amenazas son detectadas, enumeradas y se les da prioridad según las necesidades o el objetivo del atacante o del pentesting.

El modelado de amenaza consta de 4 etapas:

- Recopilar la información importante
- Identificar y darle prioridad a los activos, tanto primarios como secundarios.
- Identificar y seleccionar amenazas
- Asignación de amenazas a los activos previamente identificados.

Fase IV. Análisis de Vulnerabilidades. En este punto se debe considerar la consecución del objetivo de la estrategia escogida, esto basado en la identificación de las vulnerabilidades identificadas
.
Teniendo en cuenta esa identificación de vulnerabilidades, se debe seleccionar la táctica y herramientas a emplear para conseguir y/o alcanzar los objetivos planteados.

Fase V. Explotación: En esta fase se busca acceder a los sistemas que son objeto del ataque, para esto es necesario la ejecución de exploits contra las vulnerabilidades que se lograron identificar.

Fase VI. Post – Explotación: En esta fase tratamos de sacar el mayor provecho de las vulnerabilidades y poder alcanzar el máximo nivel de privilegios, se trata de conseguir información de la red y acceso a los servicios y datos que sean posibles.

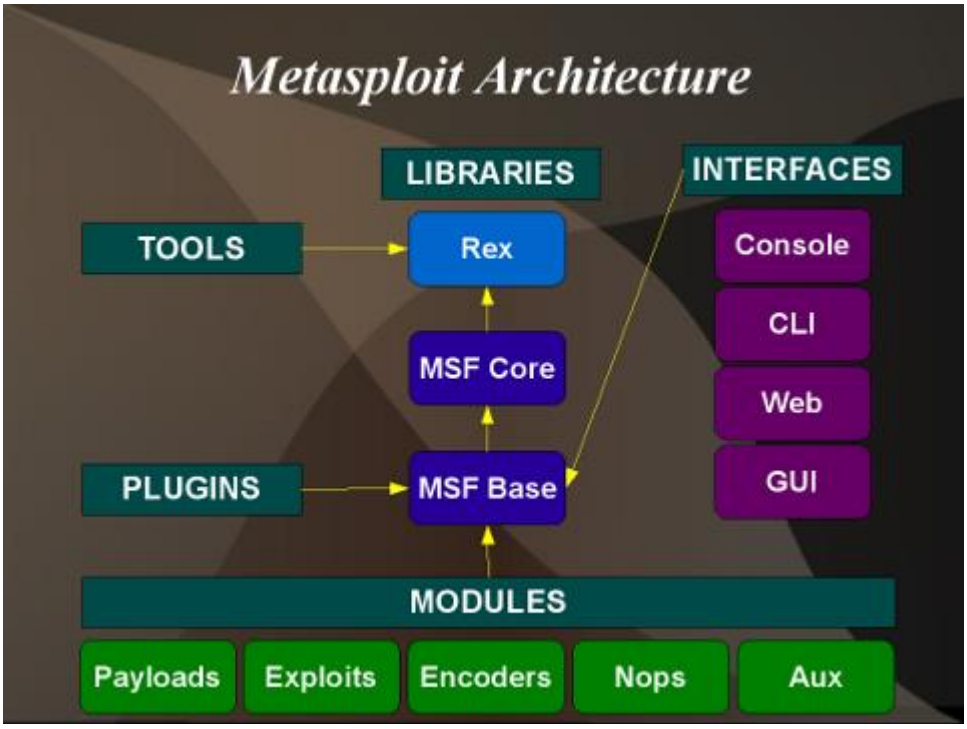
Fase VII. Reporte: En este informe se presentan los resultados de lo encontrado, se brinda información sobre los aspectos positivos y los aspectos por mejorar en cuanto a la seguridad de la organización, se debe tener en cuenta que este informe va a ser revisado tanto por personal técnico como

personal no técnico, así que lo más conveniente es que se deban realizar la entrega de 2 informes.

2.3 METASPLOIT.

Este es un software, el cual generalmente es utilizado por auditores y hackers éticos para hacer pruebas de seguridad informática, este software está compuesto por variadas herramientas, los cuales son programas pequeños, los cuales han sido desarrollados tomando como base a vulnerabilidades identificadas.

Ilustración 3. Arquitectura Metasploit



Fuente: https://platzi.com/tutoriales/1176-pentesting-2019/2224-arquitectura-de-metasploit/

2.3.1 CVE.

Es un lugar WEB que cuenta con un listado de vulnerabilidades identificadas, cada una de estas vulnerabilidades es referenciada con un código y entrega información de la fecha exacta en la que se detectó dicha vulnerabilidad, los sistemas que afectó y la forma de como contrarrestar o solucionar dicha vulnerabilidad.

Estructura

CVE-YYYY-NNNN: Identificador único compuesto por el año (YYYY) y un número secuencial de 4 dígitos (NNNN)[2].

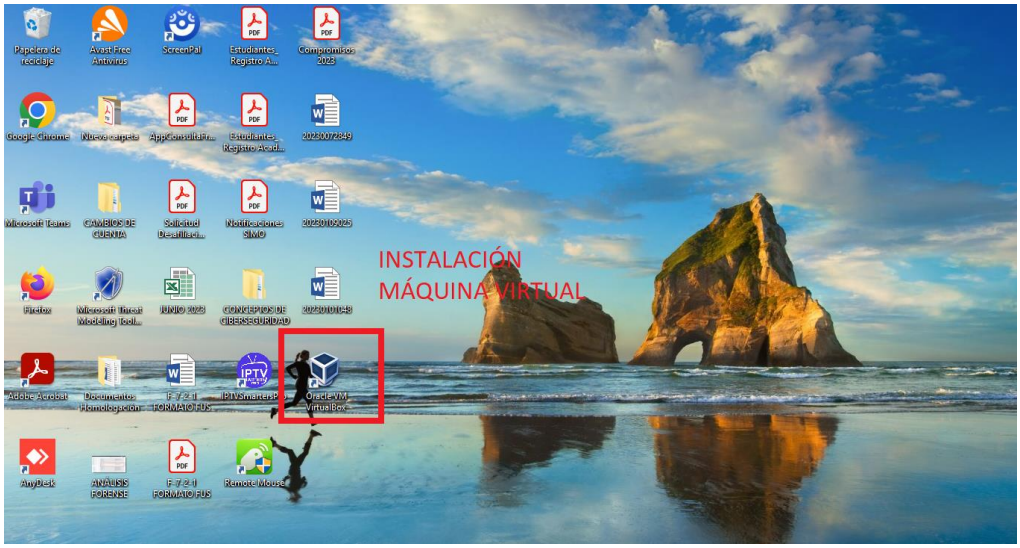
Gravedad: Las vulnerabilidades se clasificación según la gravedad, utilizando la escala CVSS, que van de 0 a 10. Cuanto más alto sea el número, más grave es la vulnerabilidad[3].

Impacto: Las vulnerabilidades se clasifican en función del impacto que pueden tener en el sistema afectado, como la integridad, disponibilidad y confidencialidad de los datos[4].

2.4 MONTAJE DE BANCO

2.4.1 Paso A: Descarga e Instalación de VirtualBox

Ilustración 4. Instalación VirtualBox

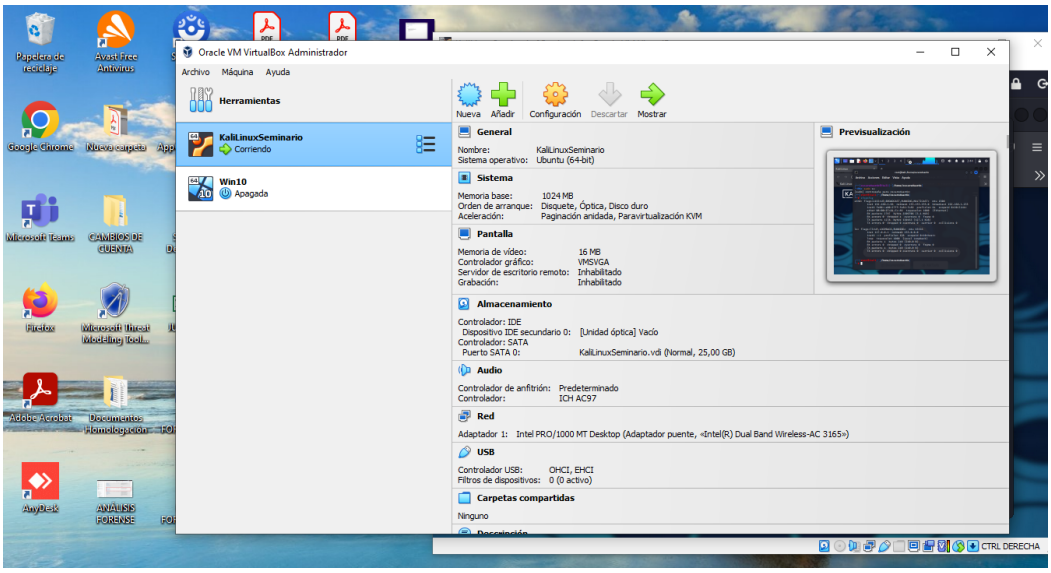


Fuente: Autor

[2][3][4] CVE y CVSS, para la clasificación de vulnerabilidades de seguridad digital. [Sitio Web]. Ostec. [Consultado: 11 de agosto de 2023]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/cve-y-cvss-para-la-clasificacion-de-vulnerabilidades-de-seguridad-digital/

2.4.2 Paso B: Configuración de 2 máquinas virtuales (Windows 10 y Kali Linux).

Ilustración 5. Máquinas Virtuales

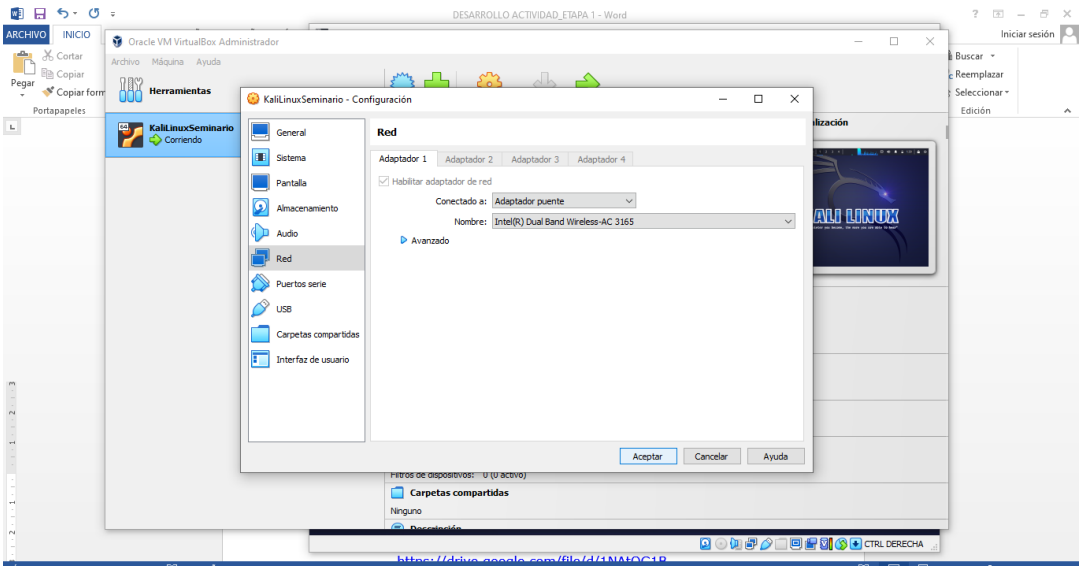


Fuente: Autor

2.4.3 Paso C: Comunicación entre máquinas

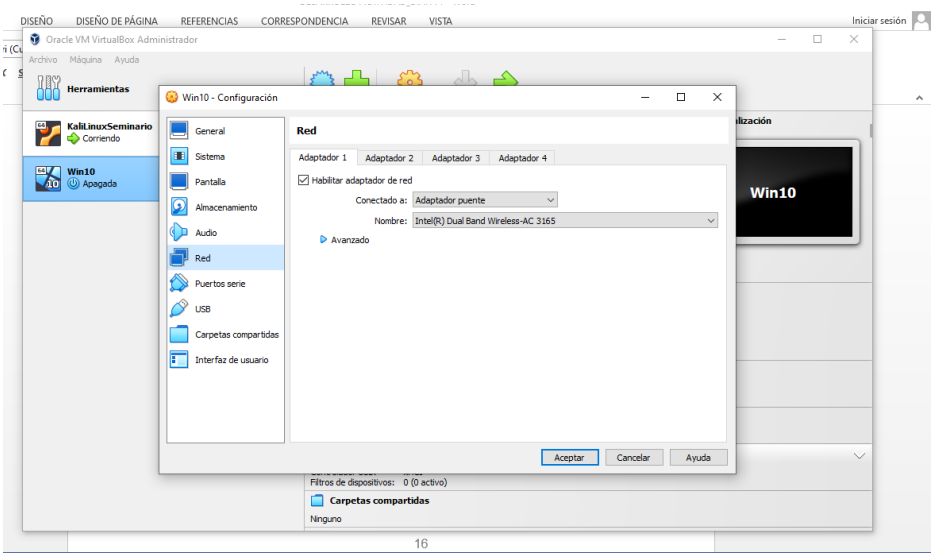
Se realiza la configuración de la RED de cada una de las máquinas virtuales en modo Adaptador Puente.

Ilustración 6. Adaptador Puente Kali Linux



Fuente: Autor

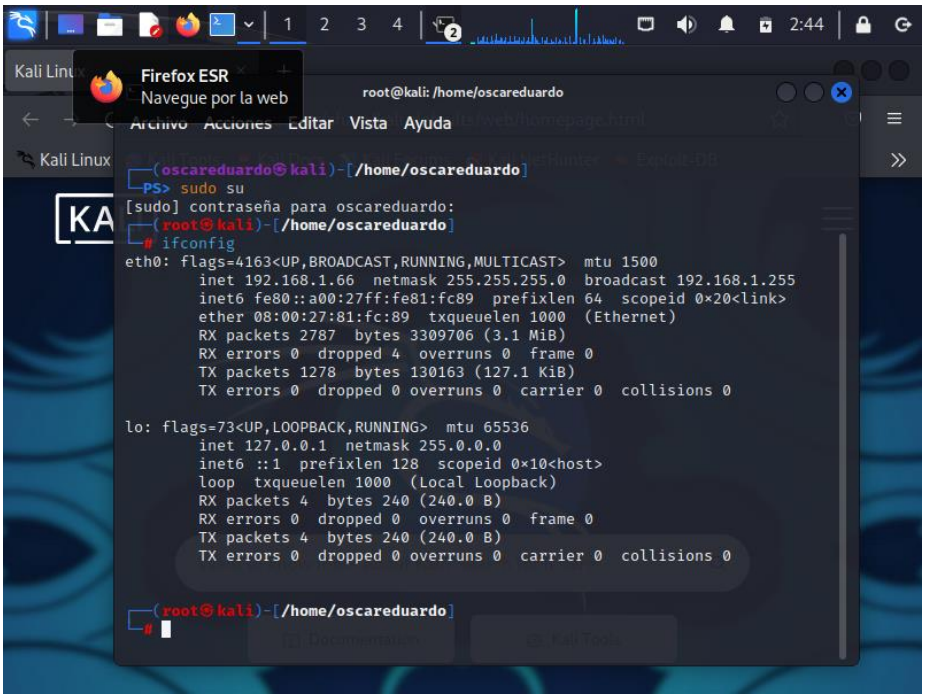
Ilustración 7. Adaptador Puente Win10



Fuente: Autor

Dirección IP Kali Linux 192.168.1.66

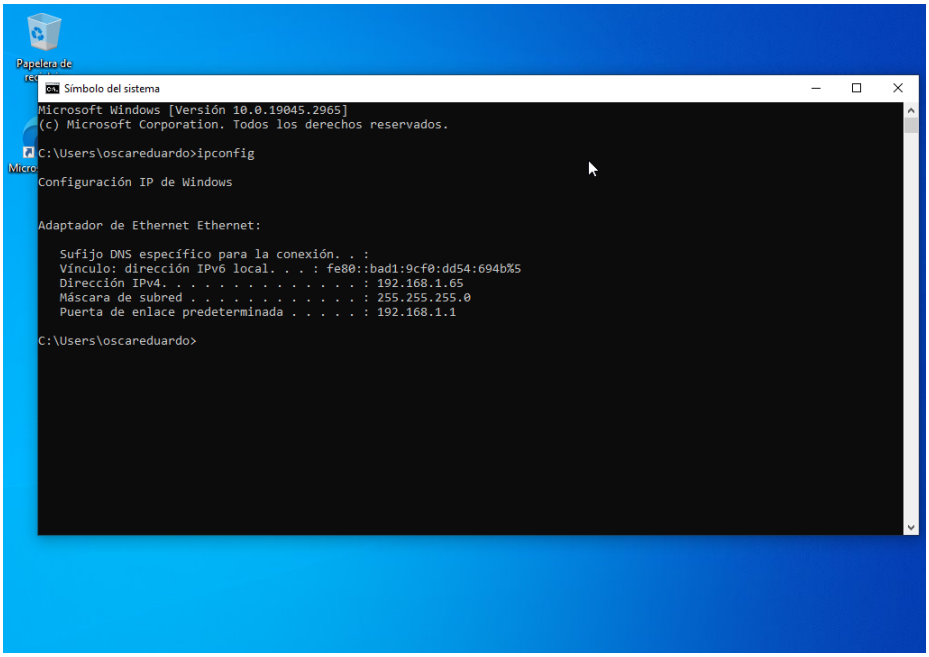
Ilustración 8. IP Kali Linux



Fuente: Autor

Dirección IP Win 10 192.168.1.65

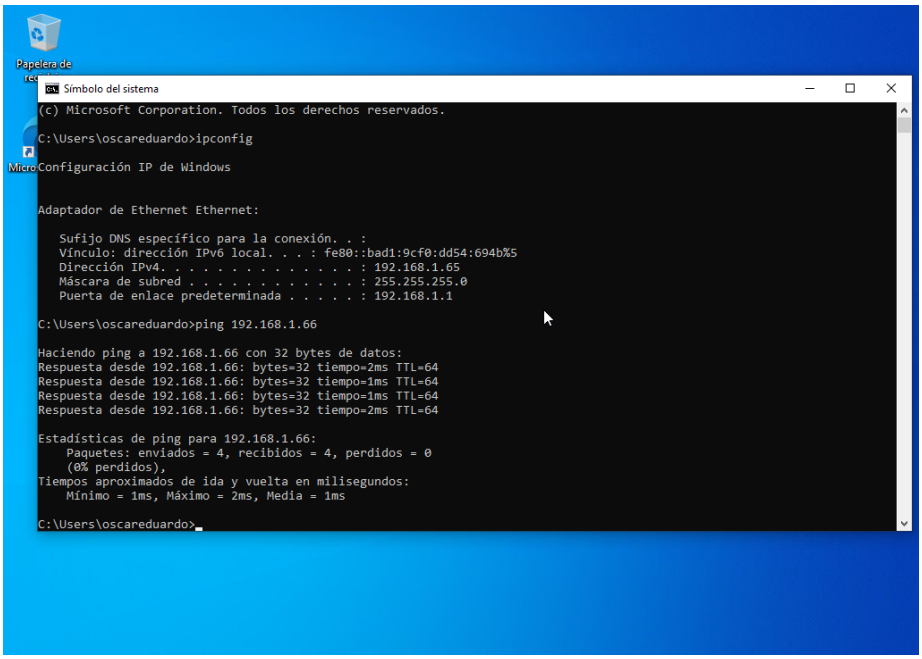
Ilustración 9. IP Win 10



Fuente: Autor

Ping de Win 10 a Kali Linux

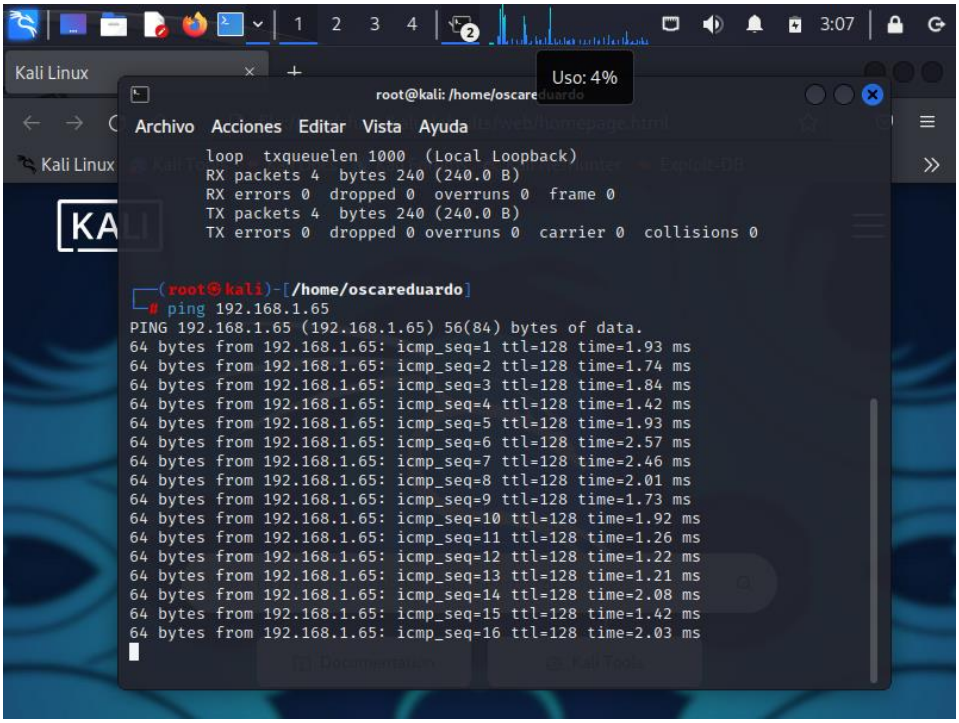
Ilustración 10. Ping a Kali Linux



Fuente: Autor

Ping Kali Linux a Win10

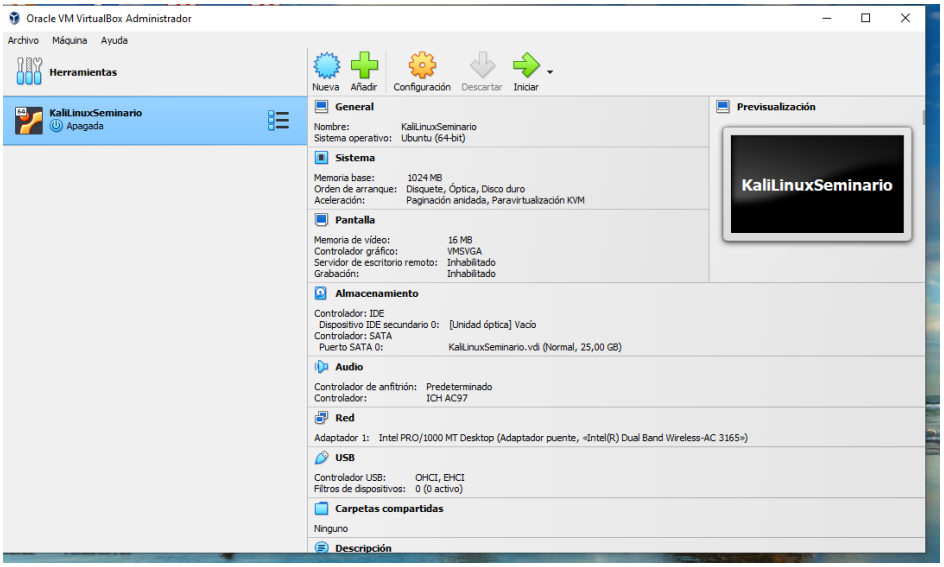
Ilustración 11. Ping a Win10



Fuente: Autor

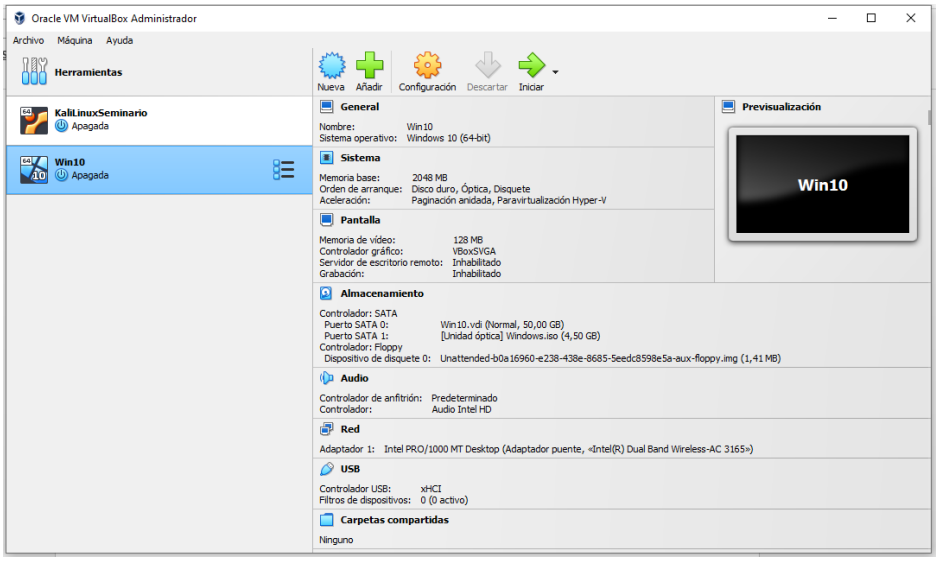
2.4.4 Paso D: Configuración Hardware Máquinas Virtuales

Ilustración 12. Hardware Kali Linux



Fuente: Autor

Ilustración 13. Hardware Win 10



Fuente: Autor

3. ACTUACIÓN ÉTICA Y LEGAL (CONCEPTO ÉTICO Y LEGAL)

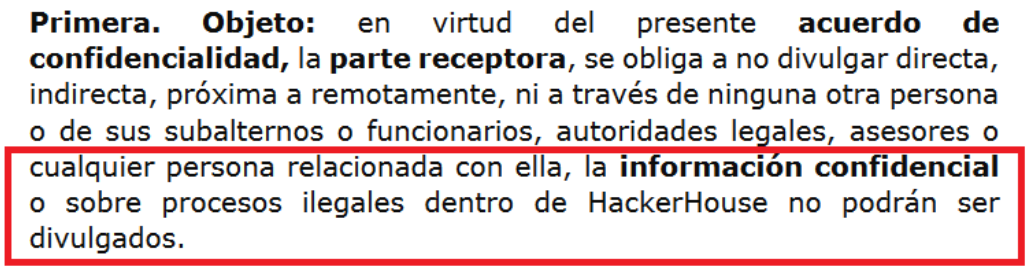
3.1 ACUERDO DE CONFIDENCIALIDAD ANEXO 3.

Una vez revisado el anexo 3 de esta actividad se pudo evidenciar las siguientes faltas eticas y legales:

Se toma pantallazo de la actividad, con el fin de evitar un alto porcentaje de coincidencias en turnitin.

En la clausula que se observa en la siguiente imagen, se puede observar que el objeto de este acuerdo contraría con lo que estipula la Ley, ya que todo acto y/o proceso ilegal debe ser reportado ante las autoridades competentes.

Ilustración 14. Clausula 1

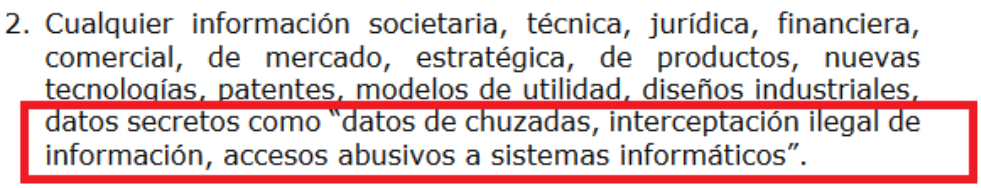


Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con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

Fuente. UNAD. Recursos Educativos.

En la clausula 2 art. 2, se puede observar como sigue habiendo complicidad por parte de la empresa con respecto a las malas practicas y se sigue contrariando la Ley, ya que se pretende acceder a información a través de medio poco eticos, sin autorización e ilegales.

Ilustración 15 Clausula 2. Art 2



2. 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".

Fuente. UNAD. Recursos Educativos.

La clausula 4 en sus art.3,4,5 y 6 "obligan" a la parte receptora a no revelar actividades o comportamiento ilegales por parte de la empresa, así mismo obliga a la parte receptora a hacerse responsable y asumir todo el peso de la ilegalidad de dichas malas practicas.

Ilustración 16. Clausula 4

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

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

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.

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**.**

Fuente. UNAD. Recursos Educativos.

En la clausula 8 resulta poco etico por parte de la empresa, que el empleado deba asumir toda la responsabilidad y dejar a su suerte al mismo por las malas practicas y malos procesos dentro de la empresa.

Ilustración 17. Clausula 8

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** 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.

Fuente. UNAD. Recursos Educativos.

3.2 PROCESO DE ILEGALIDAD ANEXO 3.

Teniendo en cuenta la Ley 1273 de 2009 se puede identificar algunos puntos que vulneran dicha Ley:

Acuerdo de Confidencialidad	Ley 1273 de 2009
Clausula. 1 Objeto. Deja ver que la información confidencial que se obtiene es realizada a través de procesos ilegales, muy probablemente violando sistemas informáticos.	Art. 269A. Acceso abusivo a un sistema informático.
Clausula. 2. Art. 2. Se mencionan "chuzadas", interceptaciones ilegales, acceso abusivo de sistemas informáticos.	Art. 269A. Acceso abusivo a un sistema informático. Art. 269C. Interceptación de Datos Informáticos. Art. 269F. Violación de Datos Personales.
Clausula. 4. Art. 3. Se debe tener en cuenta la forma en la que la empresa o a través de que medios se busca apropiar de la información de terceros, y el uso de la misma ya que se obtiene sin autorización de los titulares.	Art. 269C. Interceptación de Datos Informáticos. Art. 269E. Uso de software malicioso. Art. 269F. Violación de Datos Personales.

3.3 ANÁLISIS DE LA PROPUESTA

A pesar que la remuneración salarial es bastante atractiva, basado en mis principios personales y profesionales, mi etica y mi consiencia NO me permitirían aceptar este tipo de trabajos y mi respuesta es basada en las diferentes clausulas y articulos estipulados en el acuerdo de confidencialidad.

Así mismo, no pondría en riesgo mi tarjeta y mi ética profesional ya que dicho acuerdo contraría gran parte de lo expuesto en el código de ëtica para Ingenieros del COPNIA y mis argumentos se basan en lo siguiente:

CAPITULO II. ARTICULO 31. DEBERES GENERALES DE LOS PROFESIONALES

literal b) “ *Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su*

sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;" (COPNIA, 2023)

literal f) " *Denunciar los delitos, contravenciones y faltas contra este Código de E´tica, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;"* (COPNIA, 2023)
CAPITULO II. ARTICULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO A LA SOCIEDAD

literal a) " *Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan las incumbencia que le otorga su titulo y su propia preparación;"* (COPNIA, 2023)

CAPITULO II. ARTICULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES

literal b) " *Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones;"* (COPNIA, 2023)

3.4 NOTICIA CIBERCRIMEN COLOMBIA "ATAQUE A EPS SANITAS", IMPLICACIONES LEGALES Y ÉTICAS.

En la noticia de muchohacker.lol titulada, " Ransomhouse publica parte de información robada d keralty-sanitas y advierte que vendieron la información restante" se logra evidenciar como a través de un ransonware los sistemas de información de la EPS SANITAS fueron vulnerados, afectando el servicio de dicha entidad, así mismo hubo robo de información y datos personales de sus clientes.

Eticamente es una acción bastante reprochable ya que la entidad a la cual atacaron fue una entidad prestadora de salud, situación que afectó la atención de muchos paciencientes criticos, retrasó la autorización y entrega de medicamentos, así mismo como la autorización y realización de procedimientos e intervenciones quirurgicas.

Legalmente se presentó la información y la violación de leyes como 1581 de 2012 con el robo y comercialización de información personal de pacientes, así mismo de la ley 1273 de 2009, hubo acceso forzado y sin autorización de sistemas informaticos, uso de software malicioso[5] y hasta violación de datos personales[6].

Según lo estipulado en la Ley 1273 de 2009, las acciones anteriormente mencionadas pueden ocasionar sanciones economicas de entre 100 a 1000 SMLMV e incluso caer en pena de prisión de entre 48 y 96 meses.

Art. 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Quien de forma ilegal, es decir sin previa autorización u orden judicial intercepte comunicación electrómagnetica alguna sin importar el cualquiera de sus fases o actores, estará expuesto a una sanción de prisión de entre 36 y 72 meses.

4. EJECUCIÓN PRUEBAS DE INTRUSIÓN (PASOS Y PROCESOS RED TEAM)

4.1 HERRAMIENTAS SOFTWARE PARA EL DESARROLLO DE LA ACTIVIDAD DESDE UNA PERSPECTIVA RED TEAM.

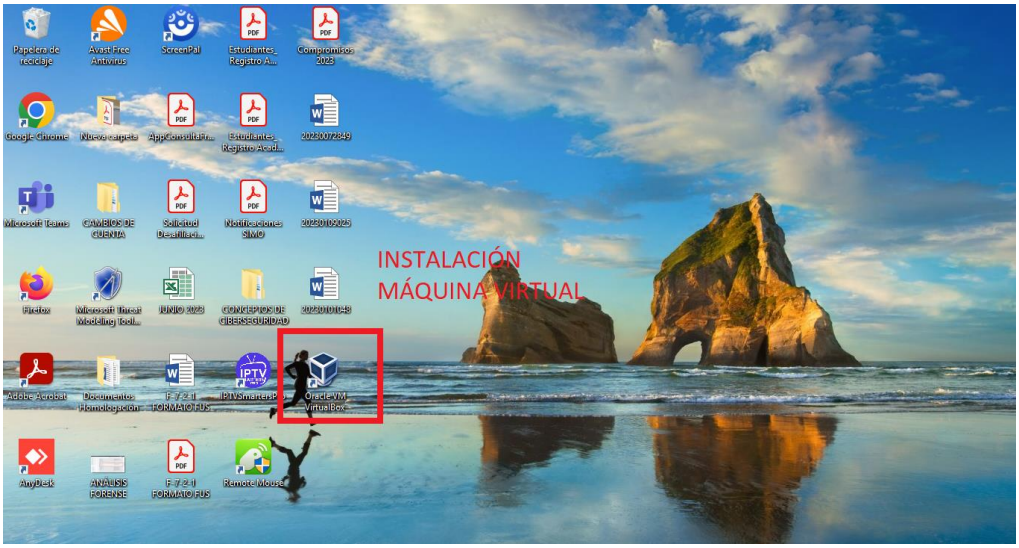
4.1.1 Máquina Virtual Box

A través de esta herramienta podemos instalar diferentes sistemas operativos en nuestro equipo, lo que brinda la posibilidad de simular ataques sin afectar el equipo de trabajo base.

La versión instalada de la herramienta es la 7.0.10

[5] [6] Ley 1273 de 2009, Congreso de Colombia. [Sitio web]. [Consultado: agosto 17 de 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ilustración 18. Máquina Virtual Instalada



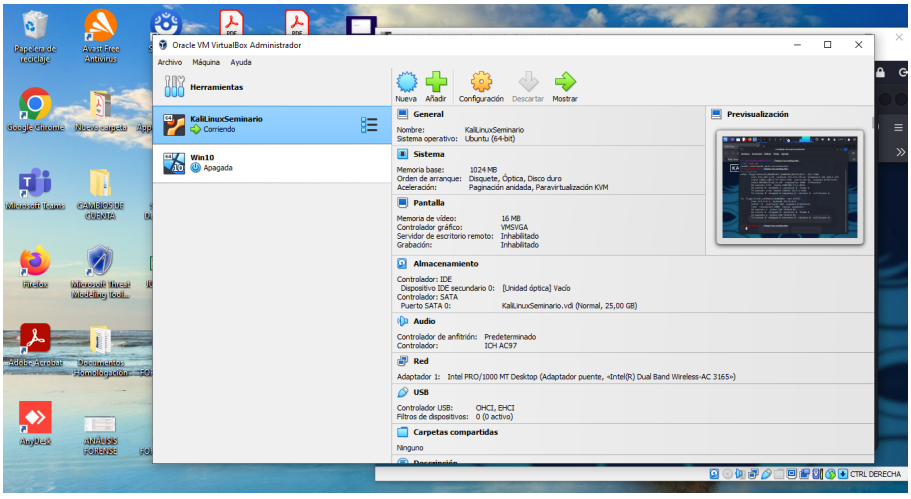
Fuente. Autor.

4.1.2 S.O Kali Linux

Como la actividad se trabaja desde el punto de vista RedTeam, hacemos mención del equipo (máquina virtual) con Kali Linux instalada, esto debido a que desde esta máquina que se va a realizar el proceso de “intrusión” a un equipo con sistema operativo Windows 10.

.

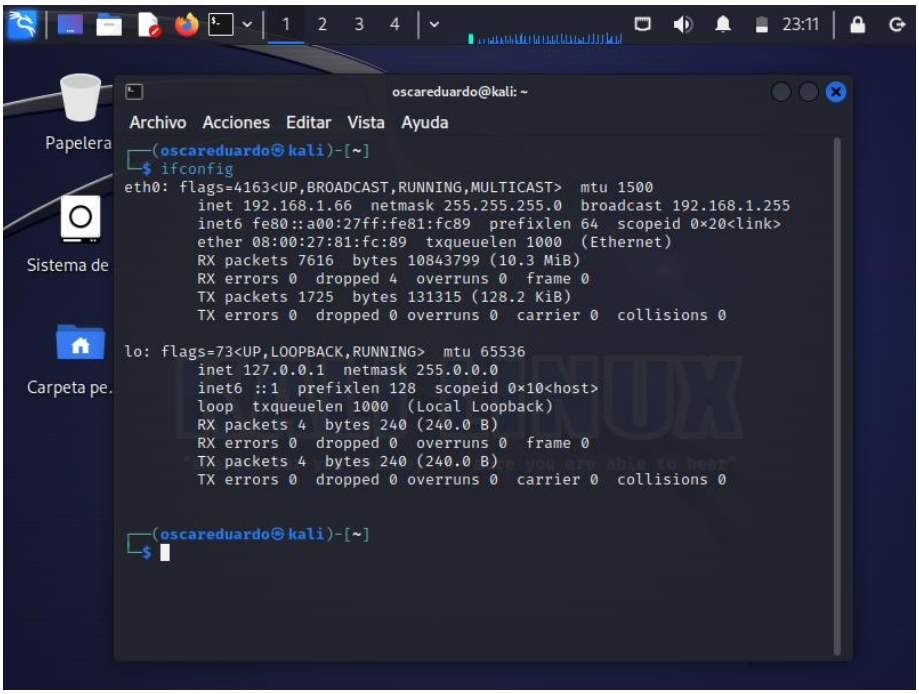
Ilustración 19 Máquina Virtualizada Kali Linux



Fuente. Autor.

Para llevar a cabo el proceso, es importante que las 2 máquinas (win y kali Linux) se encuentren en la misma red, se realiza la verificación de la Ip obtenida por Kali Linux con el comando ifconfig, IP tomada 192.168.1.66 (La IP tomada por la máquina Windows es 192.168.1.65).

Ilustración 20. Clausula 4



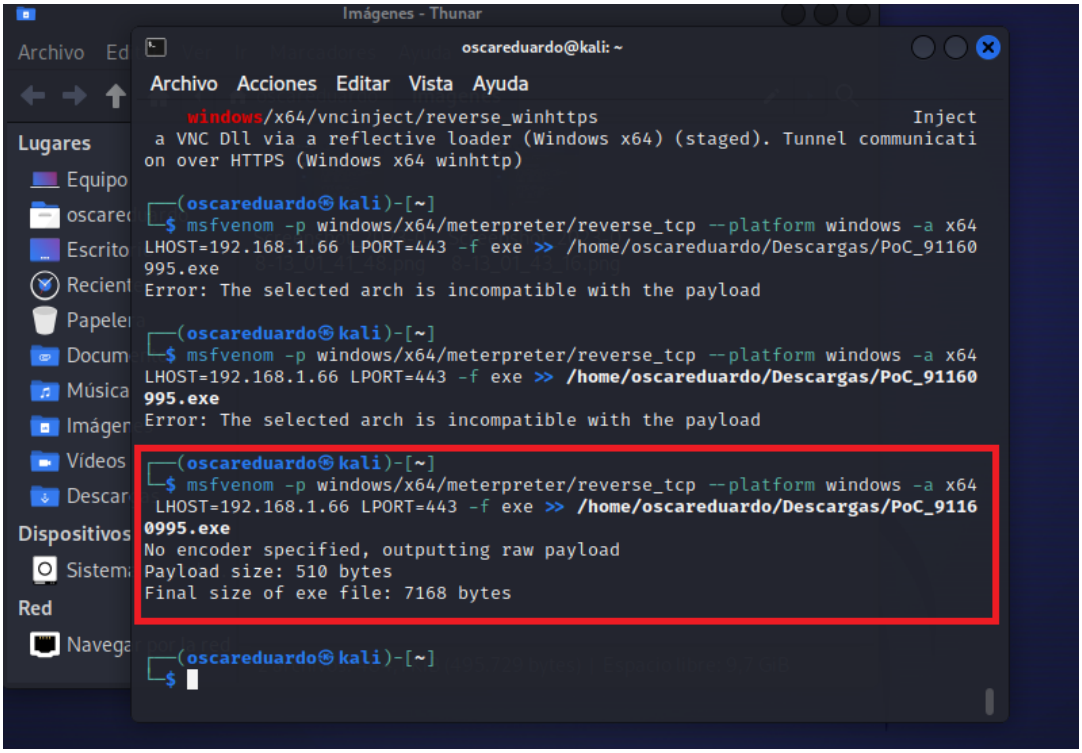
Fuente. Autor.

4.1.3 Msfvenom

Esta herramienta se empleó para crear un archivo .exe, que al ejecutarse en la máquina Windows le otorgará el control de esta al atacante.

Aquí se puede deducir que el archivo enviado por medio de whatsapp web y que tenía por nombre PocSeminario.exe fue diseñado con esta herramienta y permitió que el atacante tomara el control de la PC afectada.

Ilustración 21. Msfvenom



Fuente. Autor.

4.2 IDENTIFICACIÓN FALLOS DE SEGURIDAD ANEXO 4.

Inicialmente el anexo menciona que se ha eliminado un archivo con extensión .txt del escritorio del equipo del administrador.

Un usuario del equipo, menciona que ejecuta un archivo sospechoso, el cual recibió a través de whatsapp web, ejecutó e instala un archivo no confiable. El equipo afectado posee un S.O Win 10 a 64 bits.

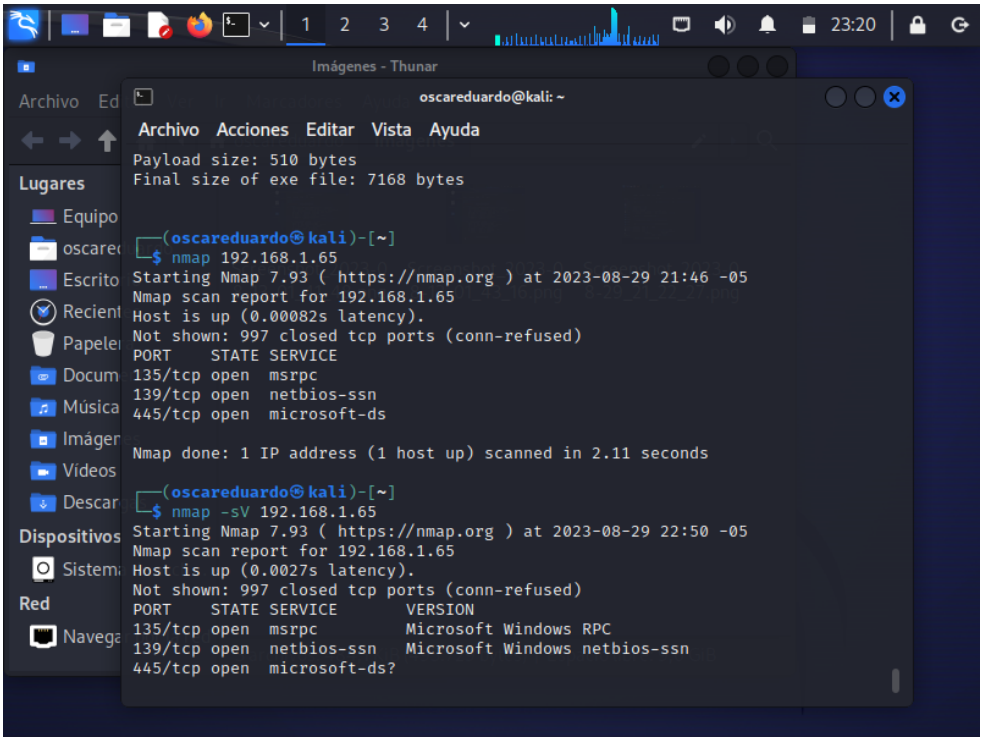
Todos los sistemas de seguridad de la máquina afectada estaban inactivos.

4.3 HERRAMIENTAS IDENTIFICACIÓN FALLOS DE SEGURIDAD

La herramienta empleada para poder identificar fallos es Nmap, ya que a través de esta, se puede realizar un escaneo de puertos y se puede identificar por donde se puede atacar o llegar a la máquina a afectar.

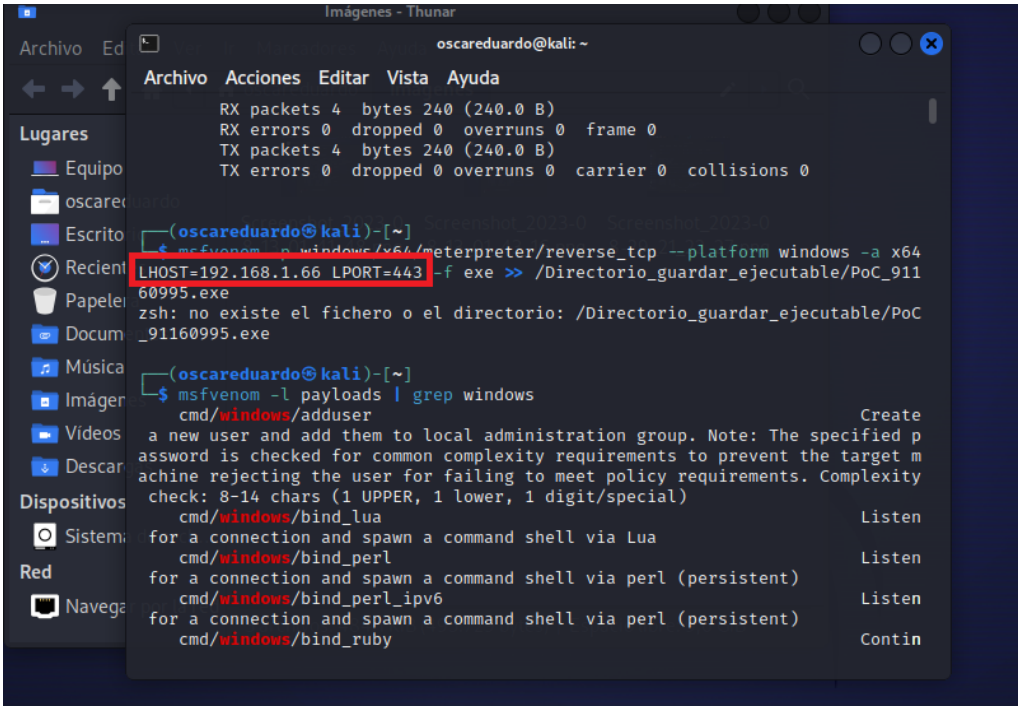
Como se puede observar, los puertos abiertos en la máquina Windows son 3 (135, 139 y 445), sin embargo para el desarrollo la actividad se hizo uso del puerto 443, el cual por defecto se encuentra abierto en la mayoría de máquinas de computo.

Ilustración 22. Código Nmap



Fuente. Autor.

Ilustración 23. Puerto Abierto



Fuente. Autor.

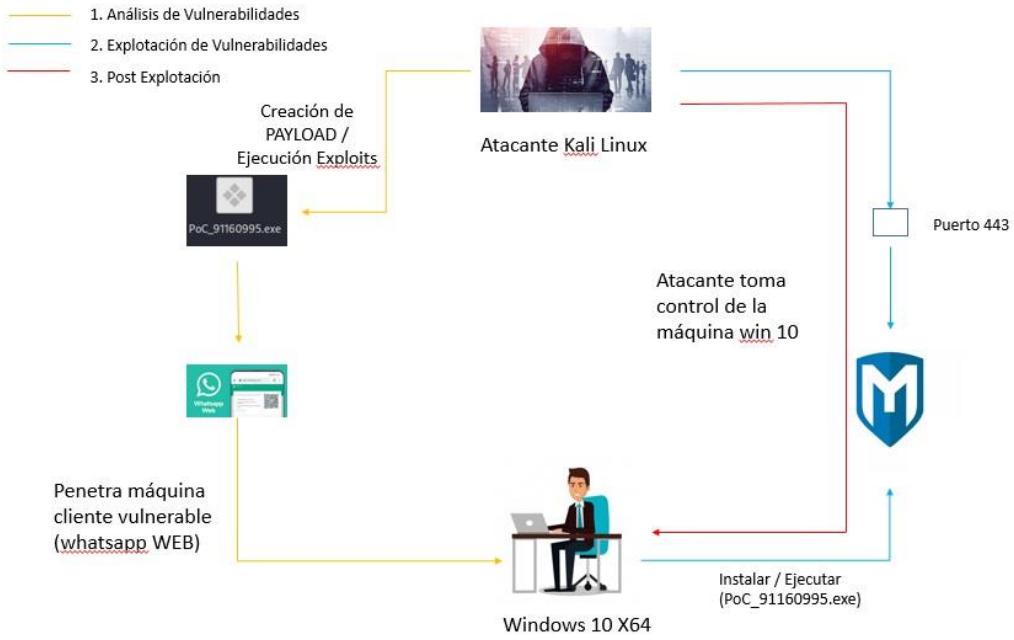
4.4 ATAQUE A MÁQUINA WIN 10 X64.

Inicialmente lo primero que hace el atacante es realizar un estudio de las vulnerabilidades del objetivo, para el caso de la actividad, se debe conocer la arquitectura y S.O del equipo objetivo, es de tener en cuenta que existe la posibilidad que el atacante deba realizar varios intentos hasta que encuentre el sistema operativo y la arquitectura correspondiente.

Luego de lo anterior se procede a explotar y/o aprovechar esas posibles vulnerabilidades, en este caso se realiza a través de la creación de un payload diseñado en Msfvenom, el cual consiste en un archivo con extensión .exe con el que se pretende sea instalado y ejecutado en el equipo víctima y esto posibilite una apertura de sesión con la máquina víctima, aprovechando el puerto 443 que generalmente siempre se encuentra abierto.

Este inicio de sesión abierto, va a permitir al atacante tomar el control de la máquina víctima por medio de metasploit, y así poder acceder a los archivos e información hasta visualizar la actividad de esta misma.

Ilustración 24. Representación Ataque Kali Linux



Fuente. Autor.

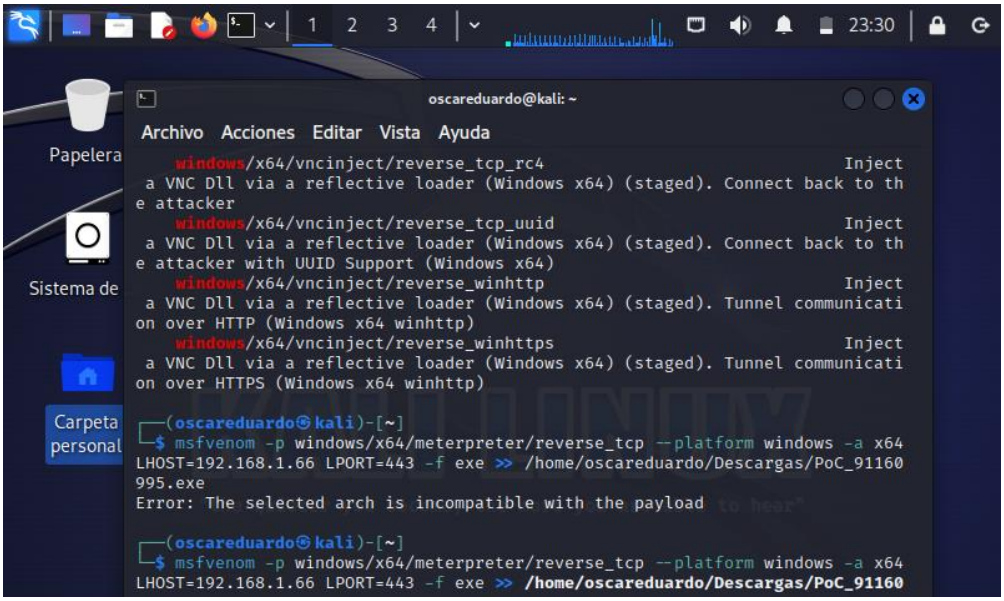
4.4.1 Afectación del ataque a la máquina.

Esta situación es muy delicada, ya que a través de este ataque un tercero pudo obtener el control total de la máquina, en este caso en particular, la situación presentada fue la eliminación de un archivo, el cual podía contener una información muy importante y muy crucial para el usuario de la máquina víctima.

La máquina está muy expuesta y vulnerable, está expuesta a fuga y eliminación de información, así mismo como violación de la privacidad.

En esta etapa se comienza a planear la forma en la que se va a penetrar o se va a atacar a la máquina víctima, en este caso se va a ser uso de los módulos existentes en metasploit (cargas útiles), los cuales se van a ejecutar en el S.O de la máquina víctima.

Ilustración 25. Carga Últil en Win 10 X64



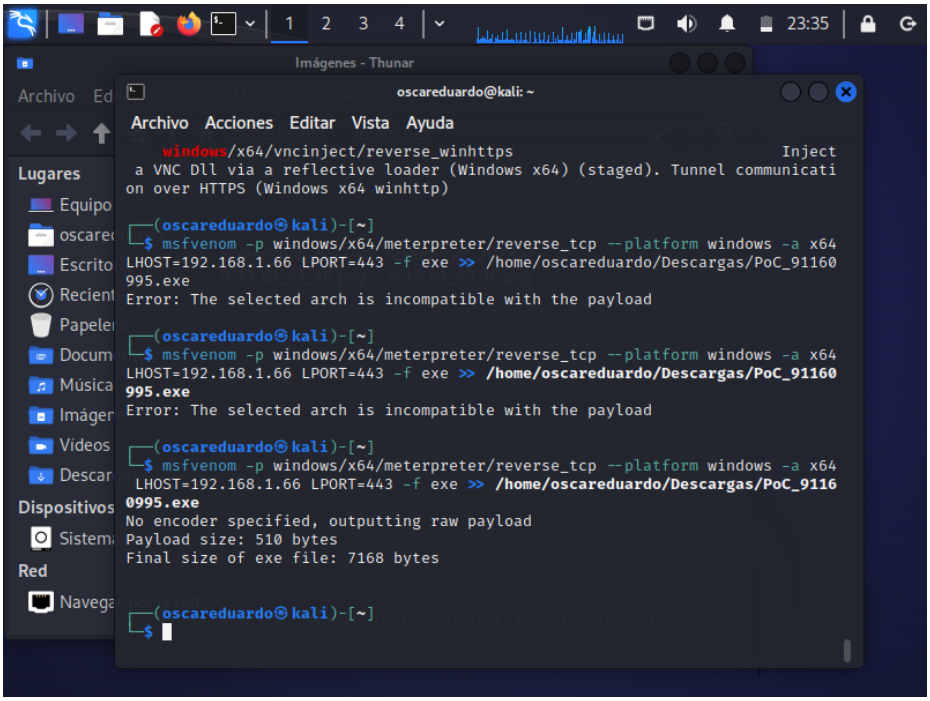
Fuente. Autor.

En la imagen anterior podemos observar, que se ha seleccionado una carga que soporte X64 de Windows 10 (máquina objeto).

Es importante tener conocimiento de los puertos abiertos que tiene la máquina objetivo, esto se realiza a través del código nmap + la ip del equipo destino, sin embargo para casos prácticos del ejercicio se va a hacer uso del puerto 443 (Ilustración 5).

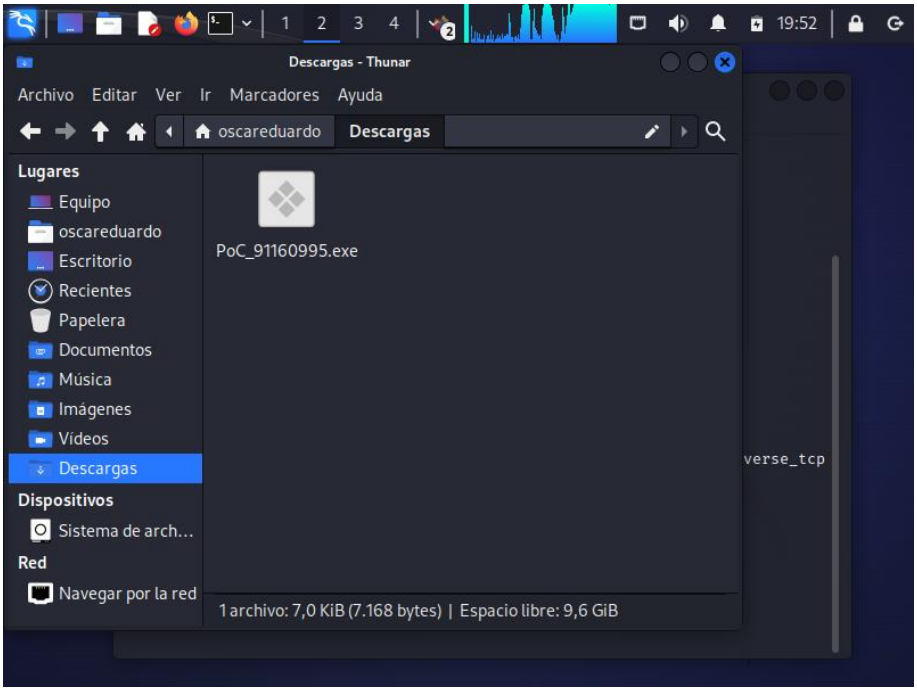
Para poder colarnos en la máquina destino, se crea un payload ejecutable .exe, el cual lleva por nombre Poc_91160995.exe.

Ilustración 26. Creación PAYLOAD



Fuente. Autor.

Ilustración 27. Ejecutable msfvenom



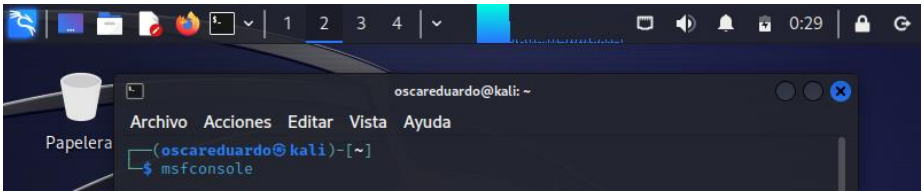
Fuente. Autor.

4.4.2 Explotación de Vulnerabilidades

La herramienta que se utiliza en esta etapa es msfconsole.

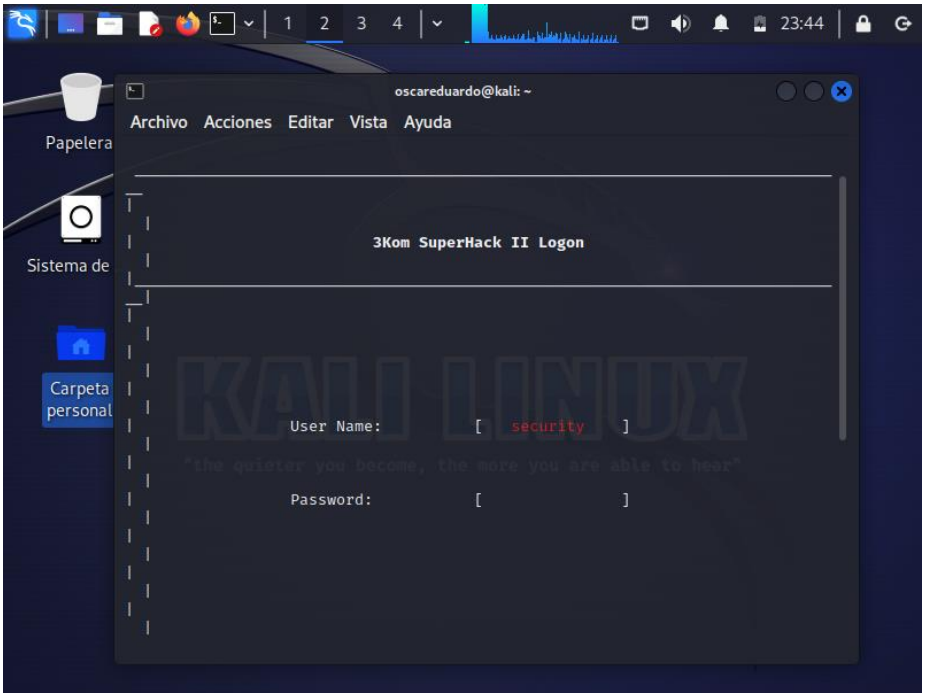
Se inicia la consola al ejecutar el código msfconsole y el comando use, para ingresar el exploit y el comando set, para introducir información del puerto por el cual se va a atacar la máquina destino, la ip de nuestra máquina anfitriona e ingresar el payload.

Ilustración 28. Código msfconsole



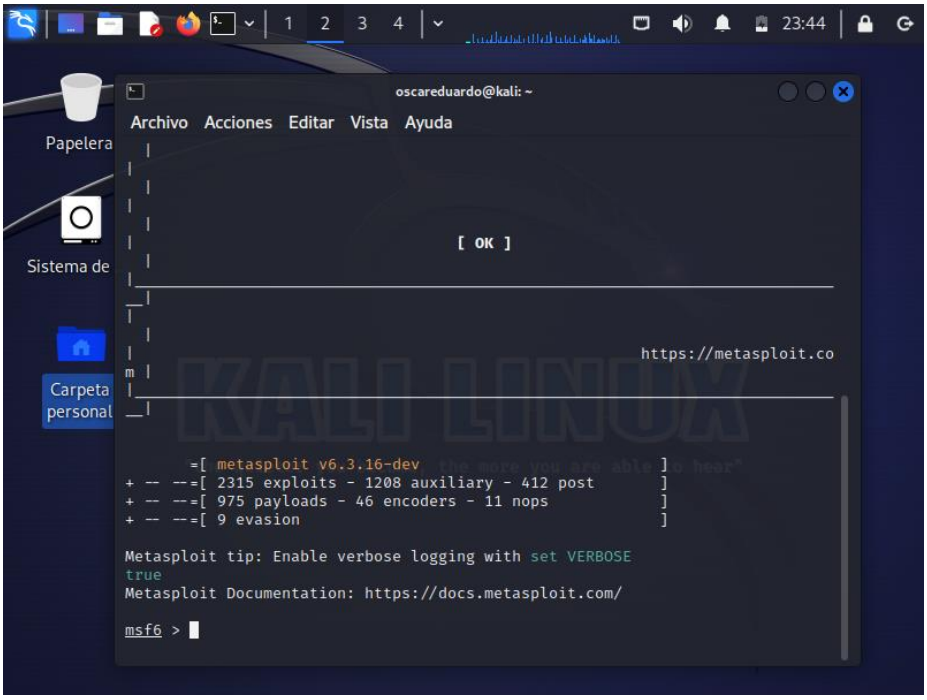
Fuente. Autor.

Ilustración 29. Interfaz Comandos Kalu Linux 1



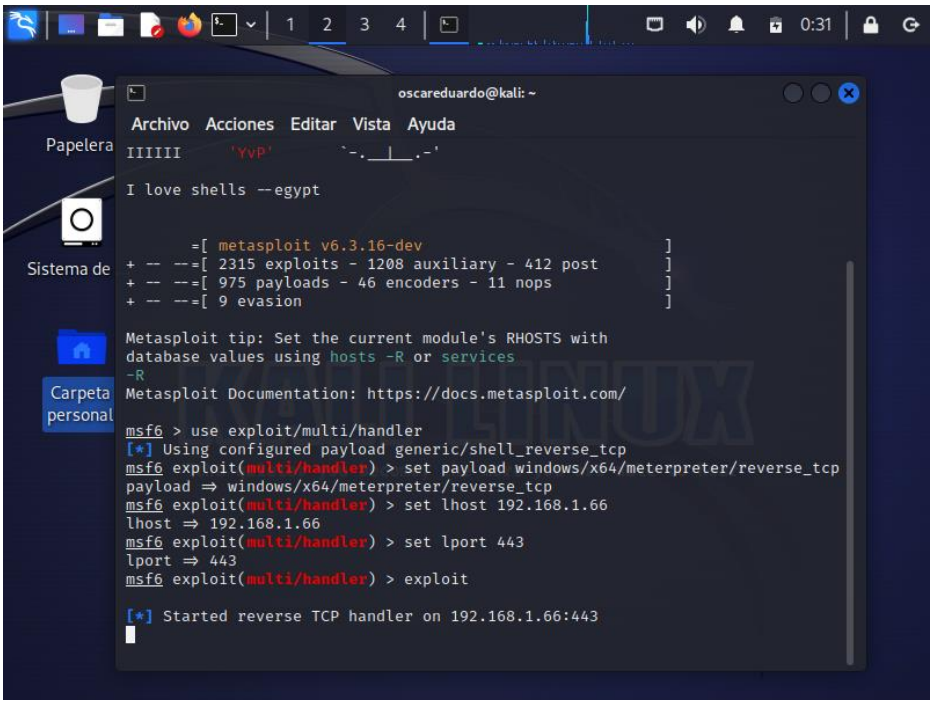
Fuente. Autor.

Ilustración 30. Interfaz Comandos Kali Linux 2



Fuente. Autor.

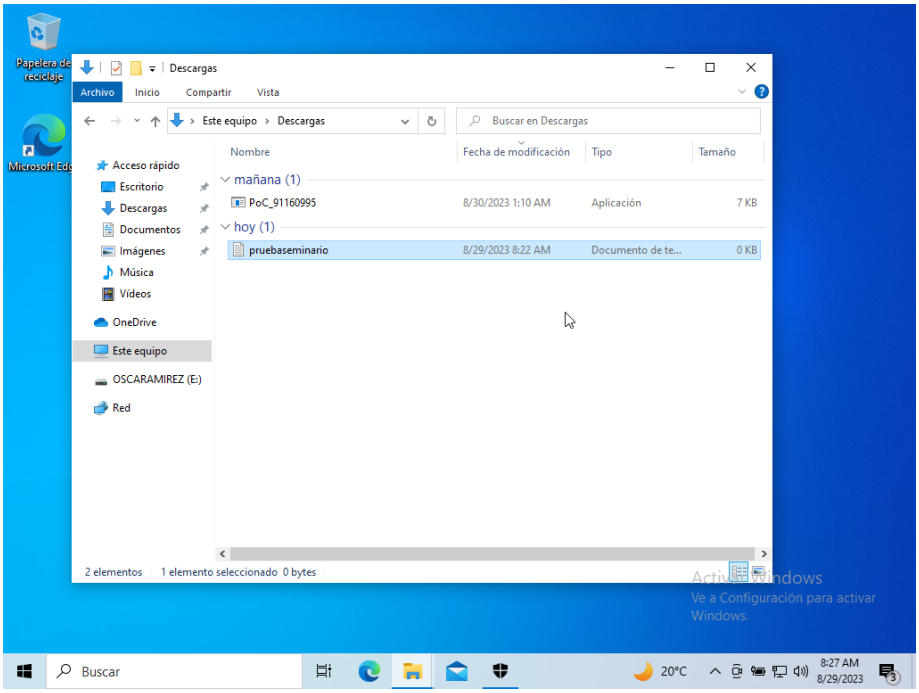
Ilustración 31. Uso Exploit / Shell Reversa



Fuente. Autor.

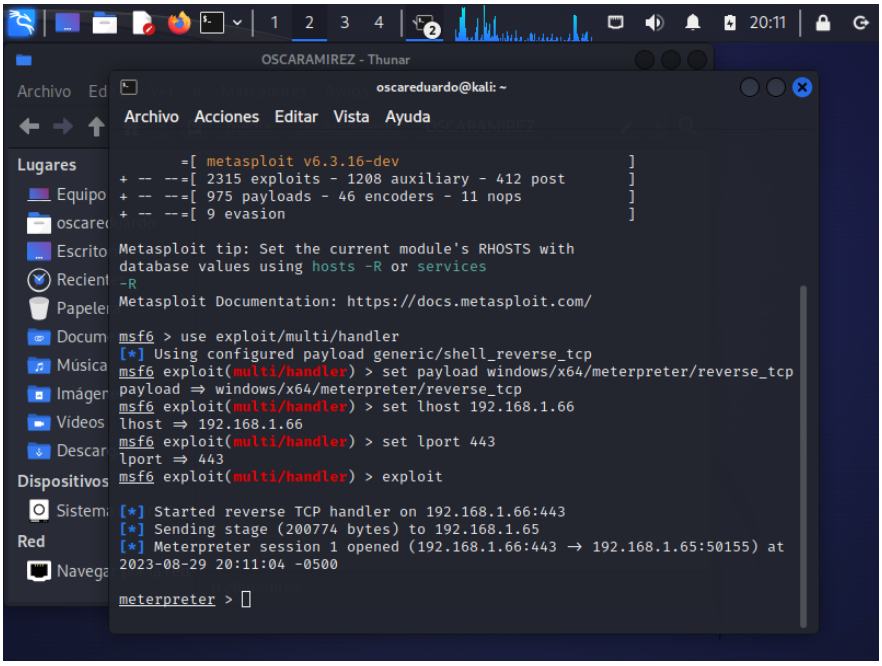
Para que el ataque sea efectivo, se debe ejecutar el archivo .exe creado, en la máquina Windows, según el caso del anexo, este fue introducido a la máquina a través de whatsapp web y posteriormente ejecutado, para casos prácticos del anexo, se copió dicho ejecutable a través de una memoria USB en la máquina Windows.

Ilustración 32. Instalación y Ejecución .exe



Fuente. Autor.

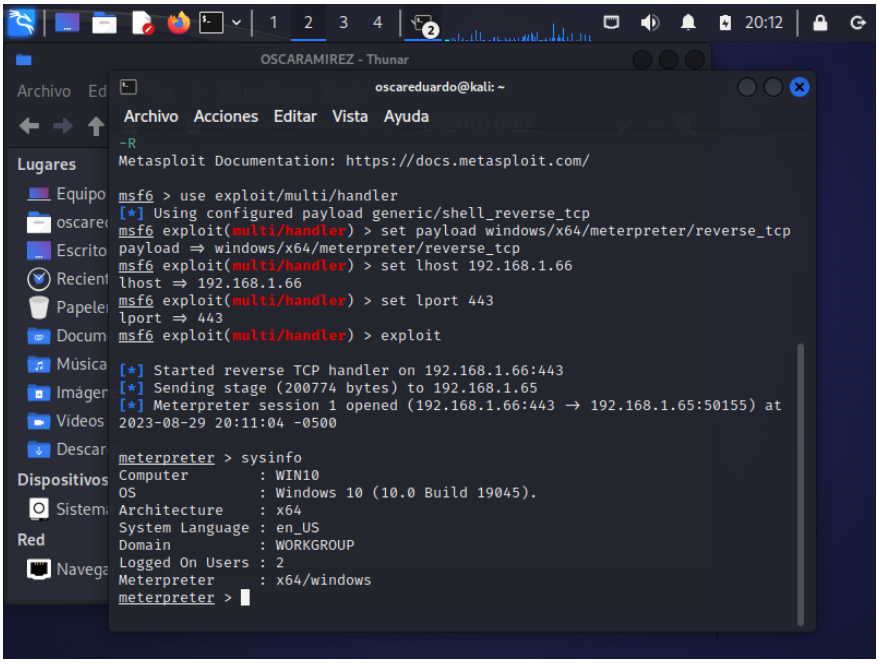
Ilustración 33. Finalización Proceso Ejecución Exploit (meterpreter)



Fuente. Autor.

Ya dentro de la máquina se verifica la información de la máquina atacada, a través del código **sysinfo** para comprobar que estamos dentro de esta.

Ilustración 34. Información Máquina Víctima

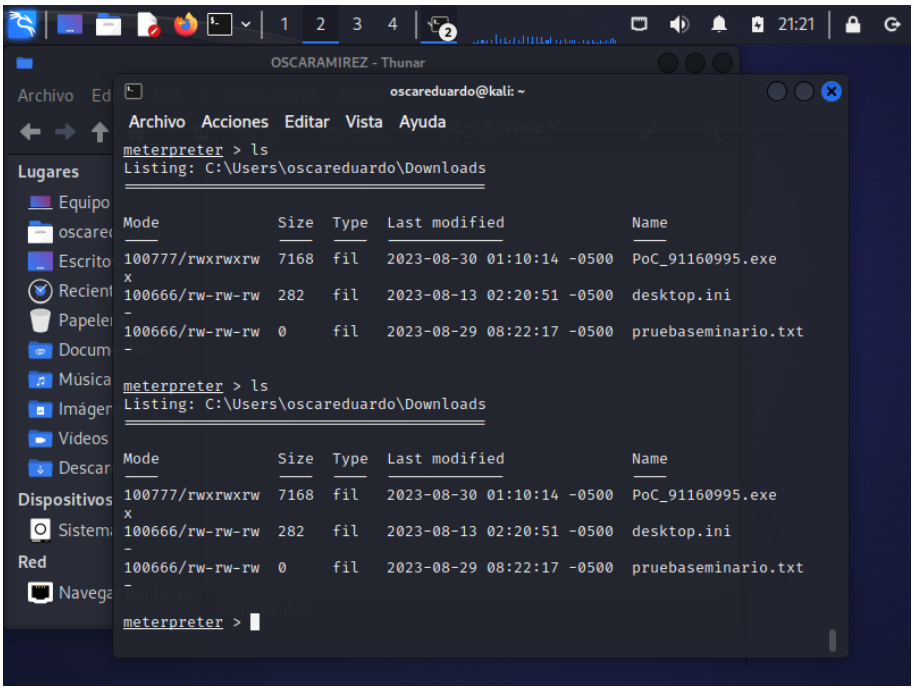


Fuente. Autor.

4.4.3 Post Explotación

Para efectos del ejercicio se debe listar y comprobar los archivos contenidos en la máquina objetivo, esto se puede realizar a través del código **ls**.

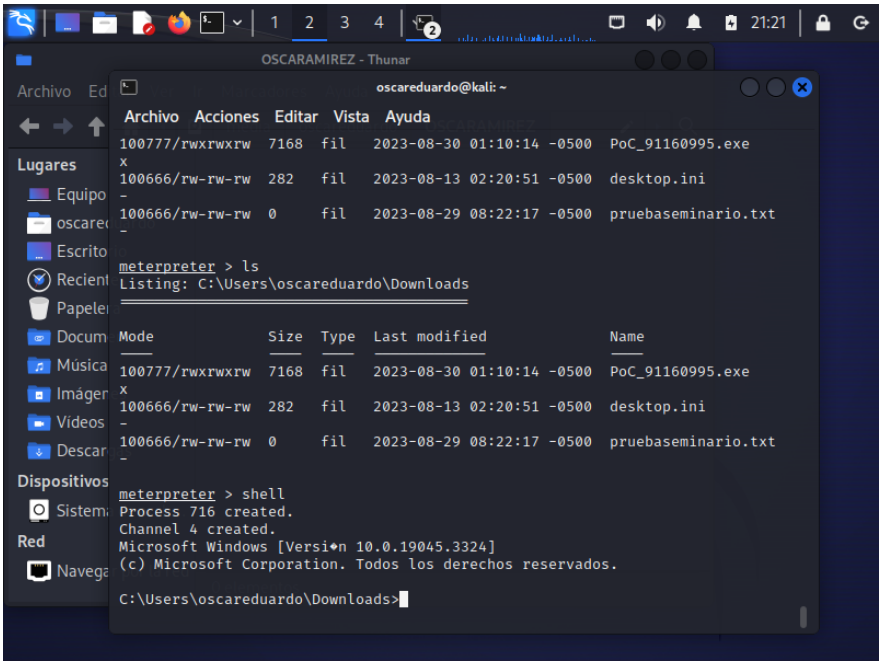
Ilustración 35. Verificación Archivos Máquina Víctima



Fuente. Autor.

A través del código podemos obtener un acceso Shell, que nos permite tomar el control de la máquina destino.

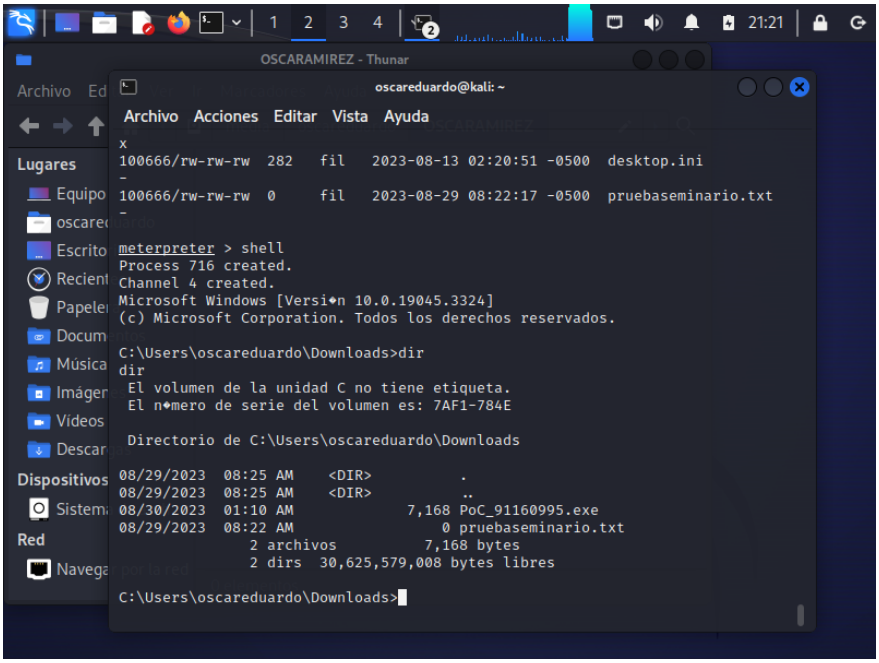
Ilustración 36. Código Shell



Fuente. Autor.

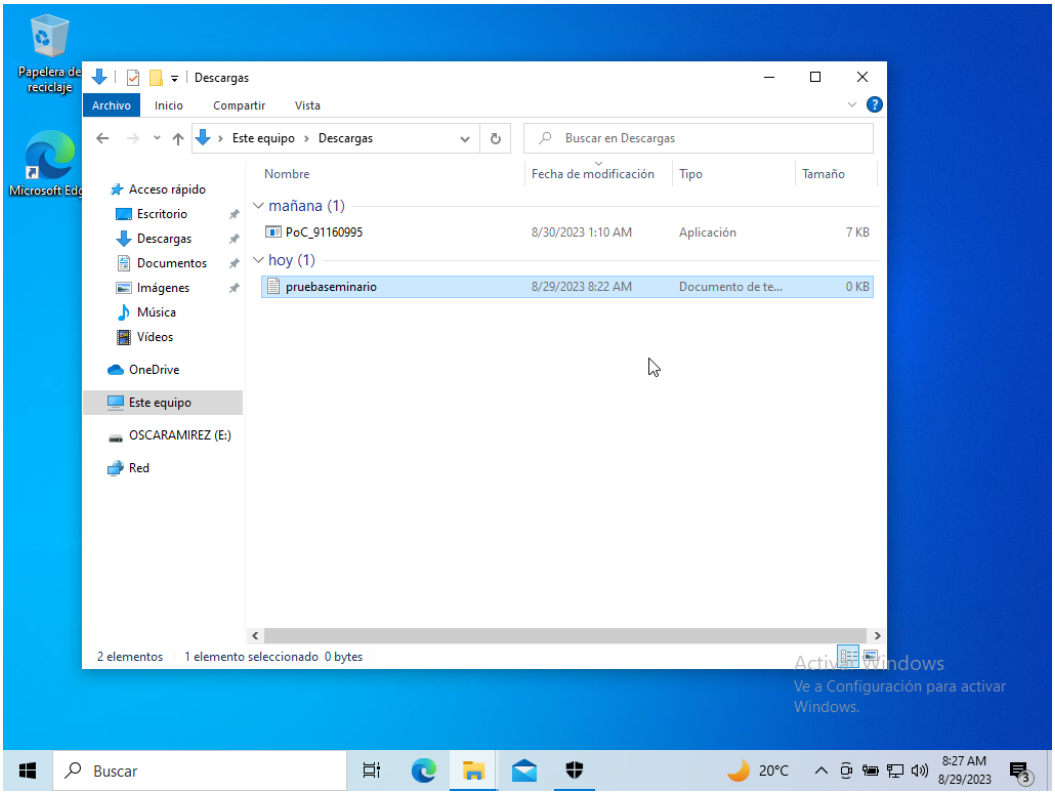
A través del comando dir, podemos observar los archivos que contienen en este caso, la carpeta descargar de Windows 10.

Ilustración 37.Archivos Carpeta Descargas Win 10



Fuente. Autor.

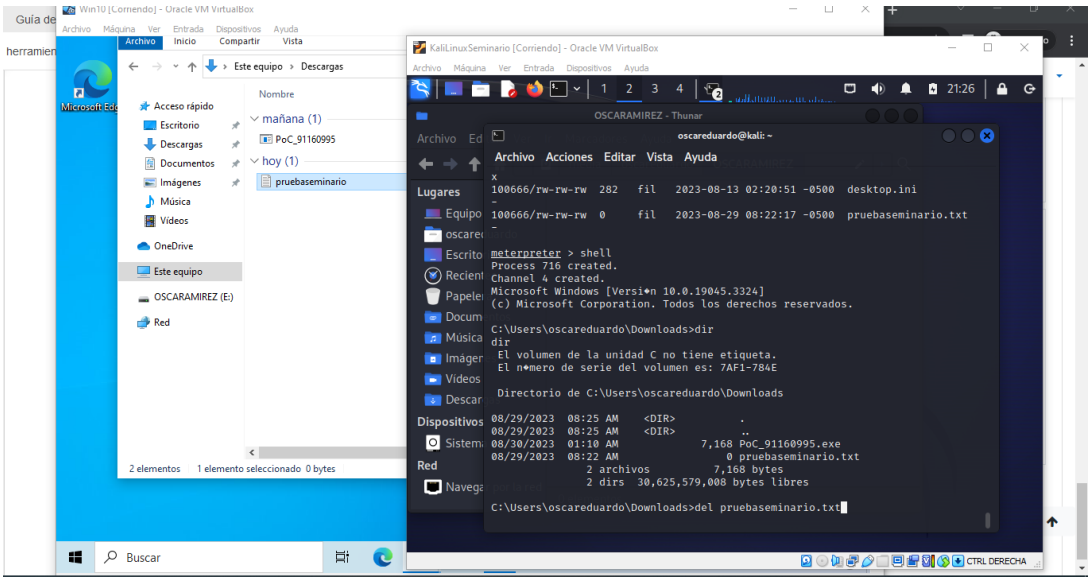
Ilustración 38. Carpeta Descargas Win 10



Fuente. Autor.

Ya teniendo el control desde la consola, vamos a eliminar el archivo .txt que tiene por nombre pruebaseminario, y esto lo podemos realizar a través del comando del. Pruebaseminario.txt

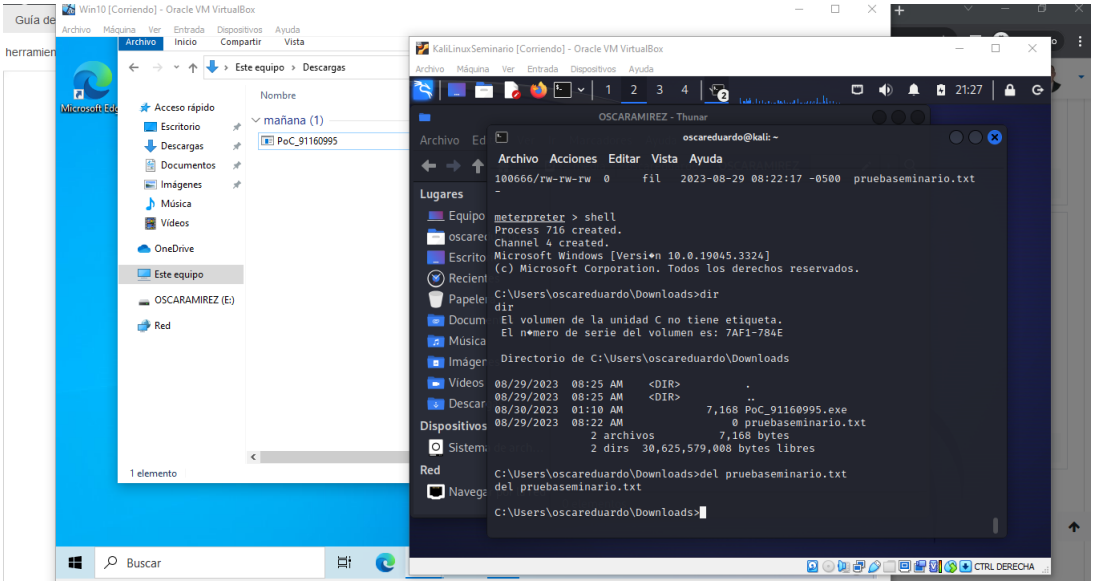
Ilustración 39. Eliminación Archivo WIN 10



Fuente. Autor.

Como se puede observar el archivo fue eliminado.

Ilustración 40. Archivo Eliminado



Fuente. Autor.

5. CONTENCIÓN DE ATAQUES INFORMÁTICOS (ANÁLISIS Y CONTENCIÓN EN BLUE TEAM)

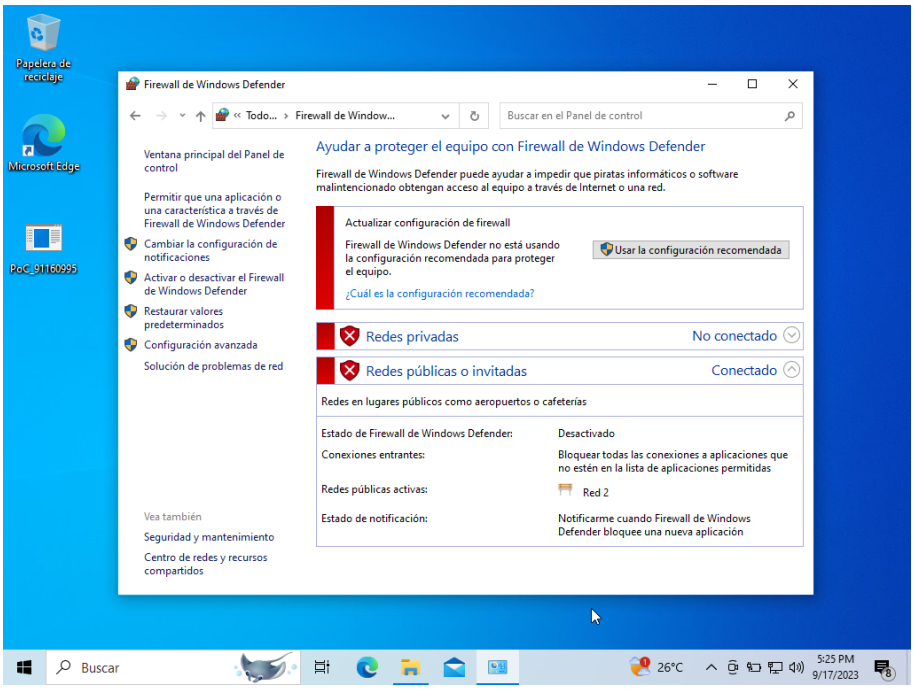
5.1 HARDENIZACIÓN HACKERHOUSE.

Tomando en consideración los diferentes artículos consultados respecto al proceso de Hardenización en Windows 10, podemos deducir que este proceso consiste en el aseguramiento y/o prevención en los sistemas contra los posible ataques informáticos esto con el fin de poder ganar tiempo por parte de los equipos de respuesta para poder tomar decisión o lograr que mitigar el impacto de dicho ataque.

A continuación se puede evidenciar el proceso de Hardenización en la máquina Windows 10 que se ha utilizado durante el proceso de este curso.

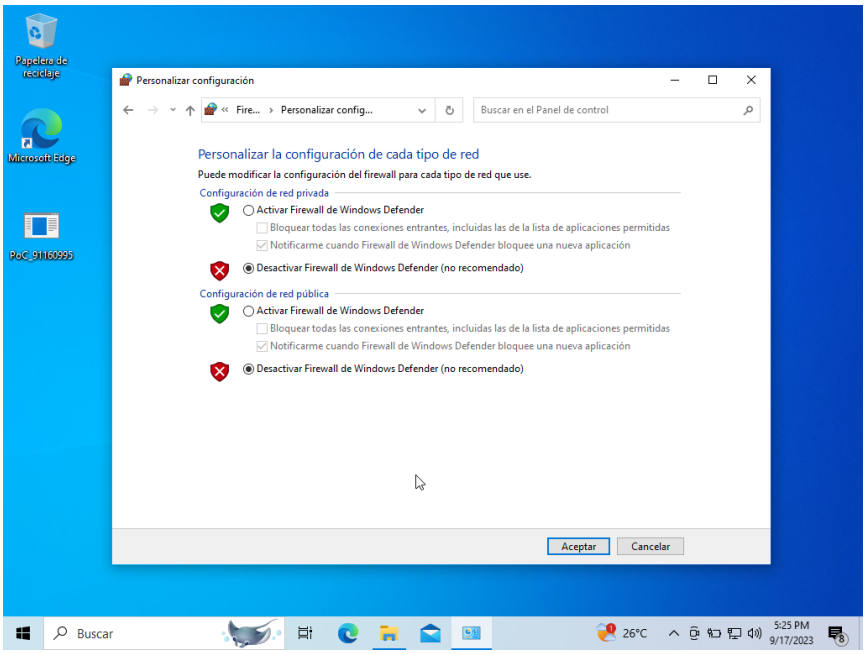
Para poder desarrollar la actividad, era necesario que todos los sistemas de prevención y/o detención de ataques en la maquina Windows estuviese abajo o desactivados.

Ilustración 41. Firewall Desactivado



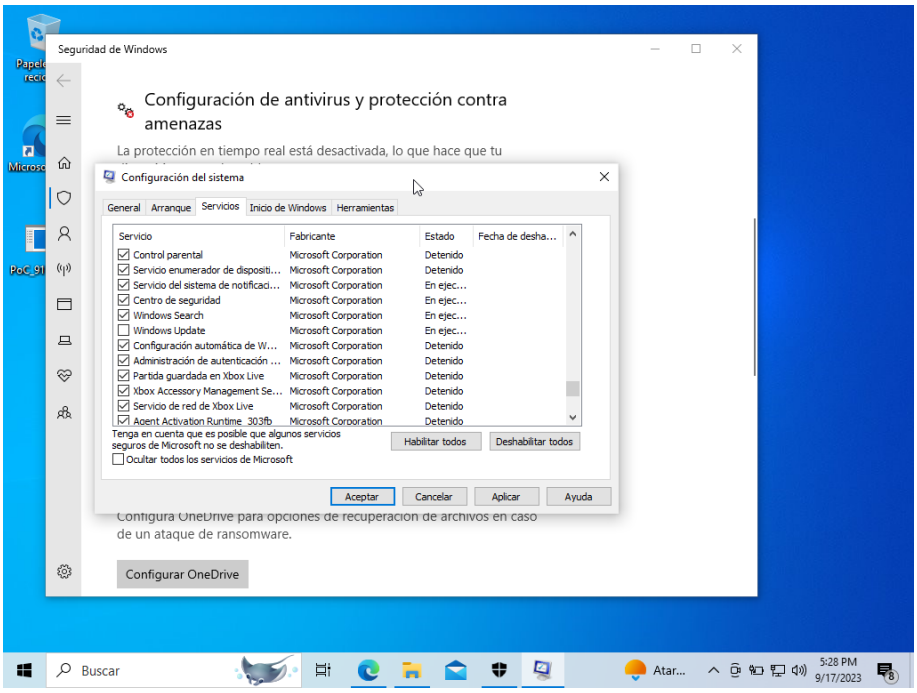
Fuente. Autor.

Ilustración 42. Firewall Inactivo



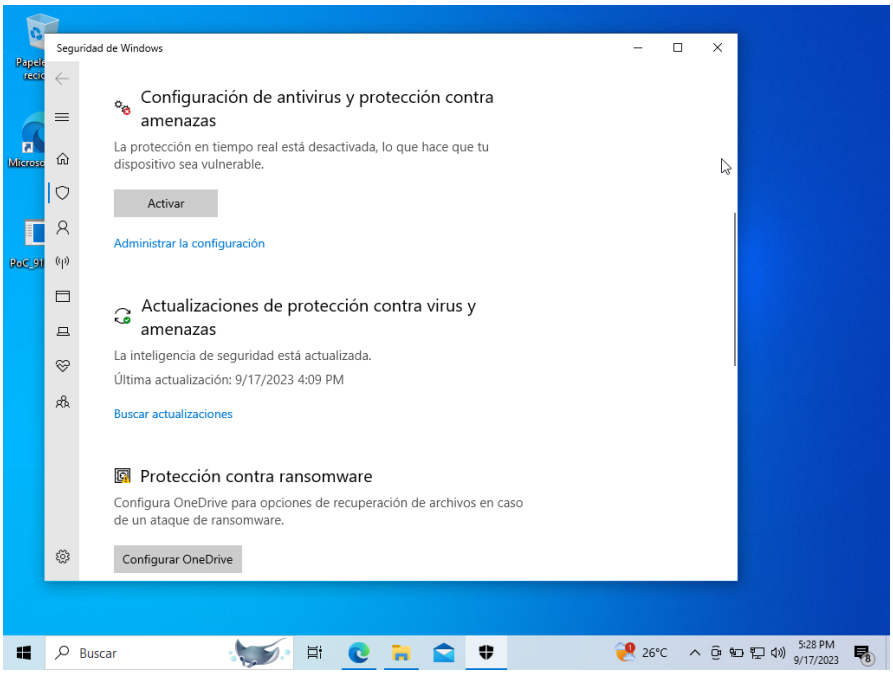
Fuente. Autor.

Ilustración 43 Actualizaciones Desactivadas



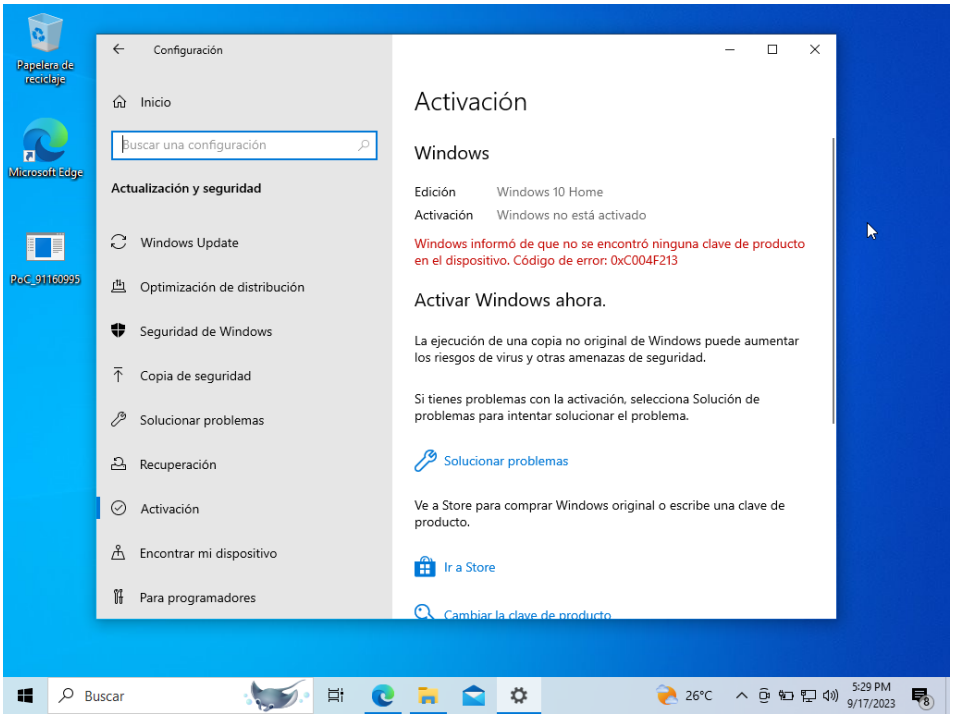
Fuente. Autor.

Ilustración 44. Antivirus Inactivo



Fuente. Autor.

Ilustración 45. Windows NO Licenciado

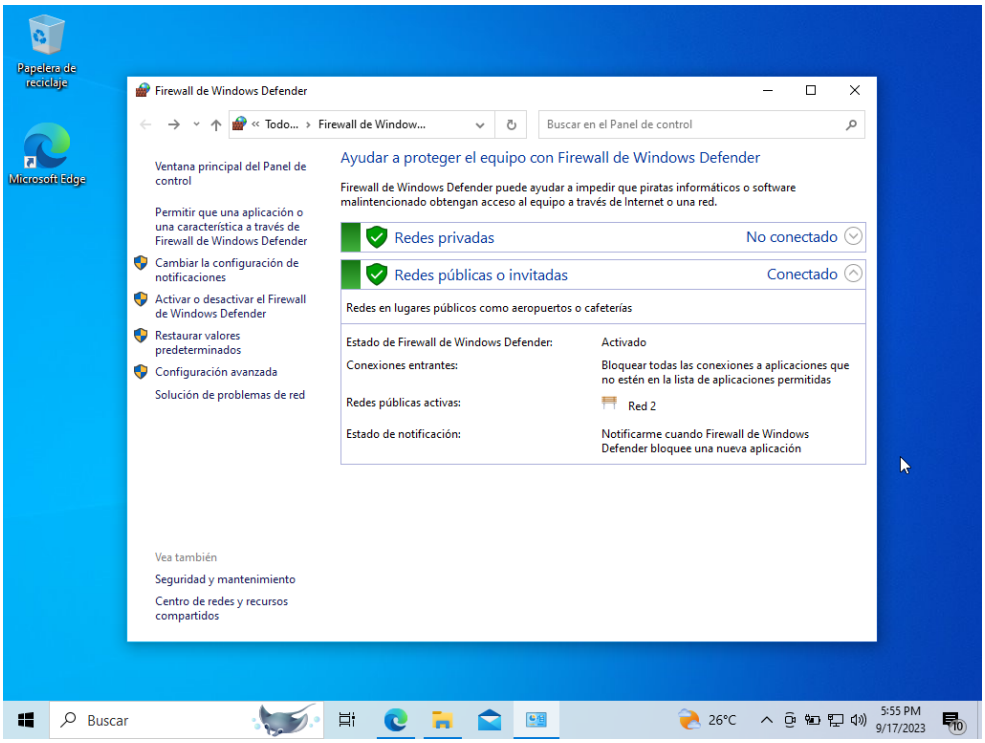


Fuente. Autor.

Para realizar el proceso de hardenización de la máquina procedemos a:

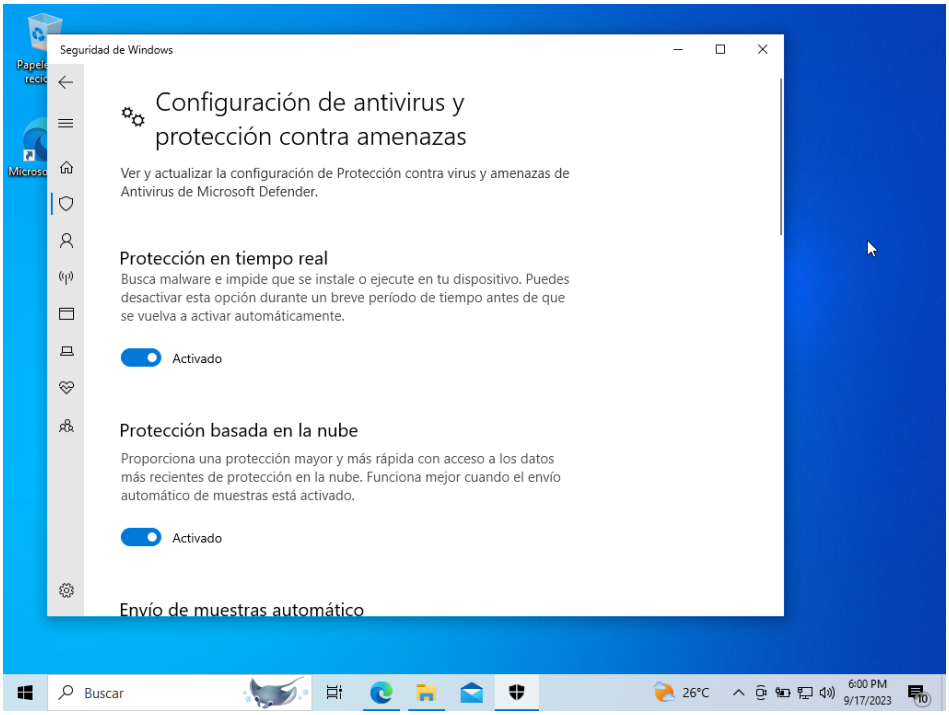
- Activación de Firewall
- Activación de Windows Defender
- Instalación de Antivirus gratuito, sin embargo lo más recomendable es que sea licenciado.
- Activación de las actualizaciones de Windows
- Tener un sistema operativo licenciado.

Ilustración 46. Activar el Firewall



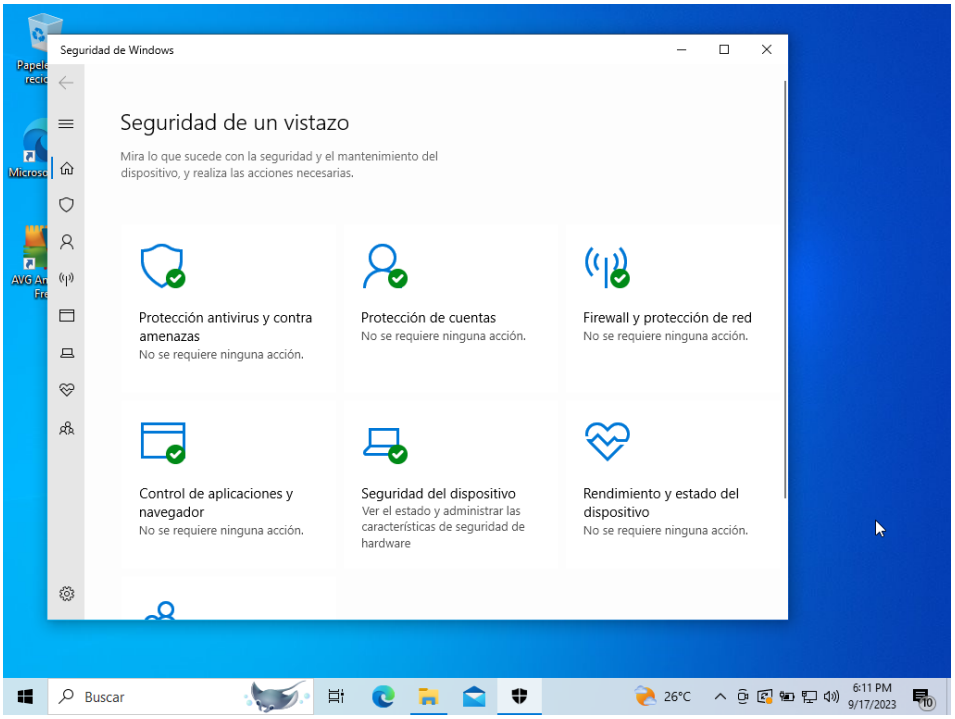
Fuente. Autor.

Ilustración 47. Activación Windows Defender



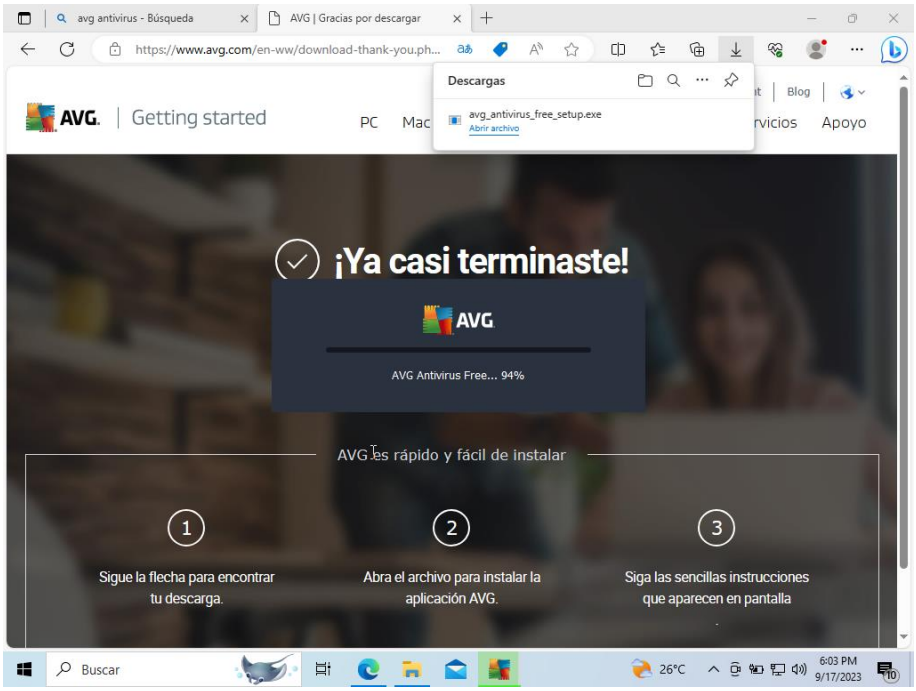
Fuente. Autor.

Ilustración 48. Windows Defender Activo



Fuente. Autor.

Ilustración 49. Instalación Antivirus

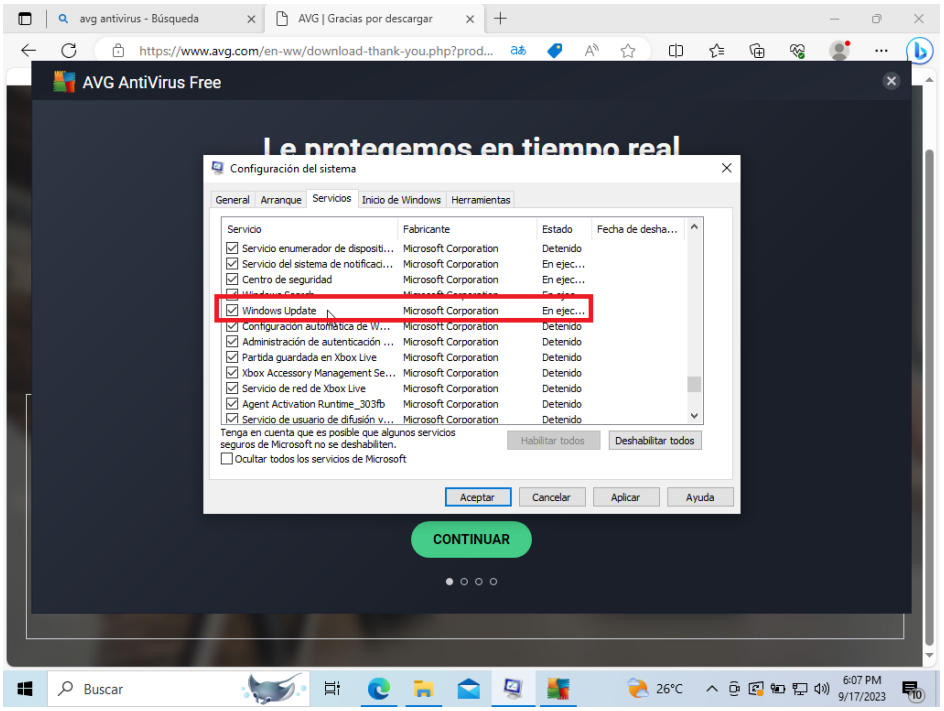


Fuente. Autor.

Ilustración 50. Antivirus Activo

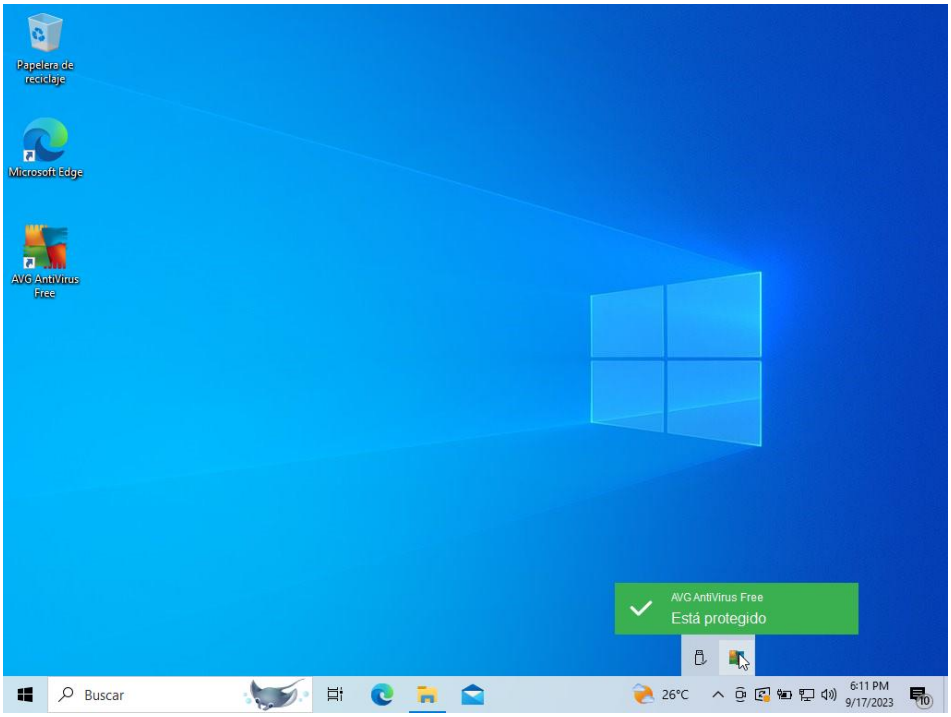
Fuente. Autor.

Ilustración 51. Activar Actualizaciones de Windows



Fuente. Autor.

Ilustración 52. Sistema Protegido

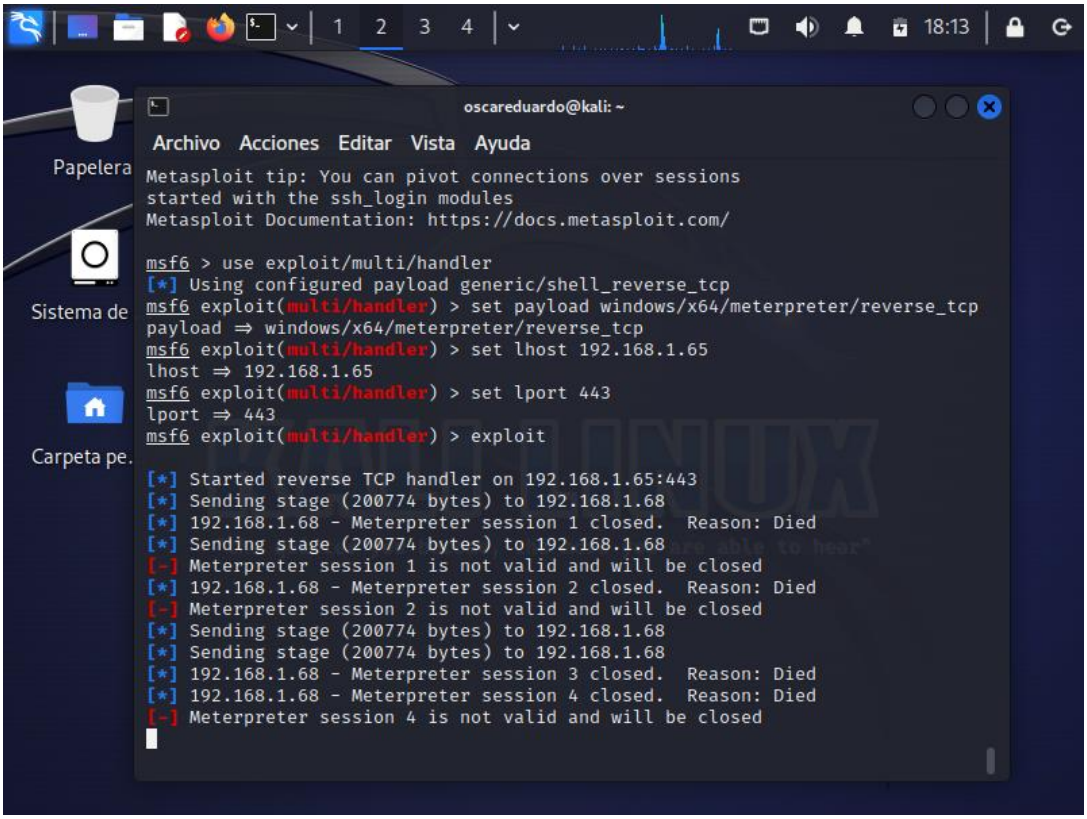


Fuente. Autor.

Tener un sistema operativo licenciado, con el fin que pueda actualizarse e instalarse parches de seguridad.

Se puede observar que luego de la instalación y/o activación de las medidas de seguridad en el equipo Windows 10, no es posible establecer conexión desde la máquina Kali Linux.

Ilustración 53. Sesión Inactiva



Fuente. Autor.

5.2 PASOS DE IDENTIFICACIÓN ATAQUE INFORMÁTICO.

Tomando en consideración el enunciado en donde se plantea que el ataque ya se ejecutó, las medidas preventivas ya no tienen caso, por lo siguiente a mi consideración se debe:

- Realizar un monitoreo constante de la red de la empresa, empleando herramientas que permita realizar esta acción así mismo como análisis profundo de la misma, lo que me va a permitir identificar que tan afectada se encuentra la red.

- Empleo de herramientas que permitan identificar los patrones del ataque, esto con el fin de poder empezar a identificar contra qué tipo de amenaza nos estamos enfrentando.
- Conformar un equipo que permita responder y/o reaccionar en forma inmediata ante incidentes.
- Aislar los equipos o parte de la red que hasta el momento haya sido afectada.

Luego de realizada la identificación y contención del ataque, se procede a realizar un análisis del porqué del incidente, que produjo el ataque y en donde estuvo la vulnerabilidad de nuestro sistema.

Se debe realizar una retroalimentación a todo el equipo encargado de la ciberseguridad en la organización, y realizar una implementación continua del ciclo PHVA, lo que nos va a permitir afianzar los controles y mejora continua en los procesos que atañen al equipo.

5.3 PASOS PARA SUBSANAR EL ATAQUE

Pasos para subsanar el ataque.

1. Lo primero que se debe realizar es culturizar a los empleados de la organización con respecto a los ataques de ciberseguridad, con el fin de poder crear una cultura de la prevención y que les permita poseer conocimientos para poder obtener hábitos positivos y buenas prácticas cibernéticas.

2. Luego de ello en el caso particular del ejemplo, debemos aislar el equipo afectado, con el fin de evitar que los demás equipos de la organización se vean afectados ya que en primera instancia no vamos a conocer de qué clase de ataque hemos sido víctimas.

3. Se extrae el disco duro de la máquina afectada.

4. Se realiza el análisis de dicho disco duro en un equipo de computado aparte, aislado de la red, lo que permite realizar un análisis en frio de este dispositivo, es importante tener en cuenta que este análisis se debe realizar sin el inicio del S.O para evitar activar el software malicioso del que haya sido víctima la máquina.

5. Se realiza el análisis de dicho duro con software actualizados para la detección virus, software malicioso, troyanos, etc.

6. Luego del escaneo, identificación y mitigación del software malicioso, se procede a iniciar el equipo con la ejecución del S.O y se activan todas las medidas de seguridad en el mismo, se realizan las actualizaciones correspondientes para que el equipo se encuentre al día en sus escudos.

7. Por último se escanea y se verifica que el equipo no haya quedado con puertos abiertos.

5.4 DIFERENCIAS BLUE TEAM, READ, PURPLE TEAM Y CSIRT.

Para poder mencionar la o las diferentes que existen entre el equipo purpura y los equipos de respuesta a incidentes informáticos en base a los equipos azul y rojo, es importante antes poder mencionar en que consiste cada uno.

Blue Team: Es la seguridad defensiva, es el equipo de seguridad encargado de defender a las entidades y/o empresas contra ciberataques.

Realiza un monitoreo constante de la red, lo que le permite analizar patrones y comportamiento anormales en esta.

Se enfoca en una mejora continua de la seguridad de los sistemas de información en las organizaciones.

Red Team: A diferencia del anterior equipo, esta seguridad es ofensiva, este equipo se encarga de emular ataques, siendo lo más similar posible a un ciberataque real, explotando los posibles vulnerabilidades de seguridad en los sistemas, esta auditoría de seguridad permite identificar que tan preparada se encuentra la organización para un ataque real y en base a esto, realizar las mejoras y correcciones necesarias.

Purple Team: Este equipo tiene la responsabilidad de maximizar la eficacia y la eficiencia en el desarrollo de las actividades correspondiente tanto del equipo azul como del equipo rojo.

Desde un punto de vista personal, es como un puente de comunicación entre los equipos rojo y azul, en donde facilita la labor de compartirse información entre estos dos equipos, realiza una coordinación de las actividades entre los mismos.

Ilustración 54. Cuadro Equipos Seguridad

Fuente: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

Equipos de Respuesta a Incidentes Informáticos (CSIRT): Este equipo como su nombre lo indica, presta el servicio de respuesta a incidentes, es decir, entra en acción cuando la incidencia o el ataque se está ejecutando, en donde su objetivo es el análisis de la situación (incidente), responder y mitigar dichas amenazas para que el impacto sea el menor posible dentro de la organización.

Así mismo este equipo tiene como objetivo identificar o detectar el rastro de dicho ataque, a través de que vulnerabilidad se efectúo el mismo, por eso realizan el análisis forense del incidente, investigan una posible nueva amenaza y se encarga de coordinar las acciones legales a tomar debido al ataque.

Ahora bien, tomando en consideración las definiciones anteriormente descritas, podemos deducir que los equipo base, blue y red team tienen como finalidad la prevención y la explotación de vulnerabilidades respectivamente, dentro de un ambiente controlado, basados en auditorias de ciberseguridad, a diferencia de los CSIRT que actúan en casos reales cuando un ataque se está llevando a cabo con el fin de contener dicho ataque y mitigar el impacto de dicho ataque en la organización así como de realizar un análisis forense de para lograr identificar el origen y secuelas del ataque.

Desde el punto de vista de purple team, considero que más que diferencias marcadas contra blue team y red team es un complemento que permite que estos equipos se potencialicen, se documenten y se organicen para que el desempeño de sus funciones sean cada vez más eficientes, eficaces y más cercanas a la realidad.

5.5 FUNCIONES CIS.

Que es CIS.

Centro para la seguridad de Internet, es una organización la cual tiene como finalidad afianzar los conocimientos, preparar de mejor manera la respuesta en cuanto a la ciberseguridad por parte del personal tanto el sector público como privado.

Dicha organización trasmite o comparte dichos conocimientos y/o tips a través de correos electrónicos, videos, documentos on line, guías, infografías en donde se suministra información y consejos sobre ciberseguridad, así mismo brinda asesorías para que las entidades puedan desarrollar sus políticas de ciberseguridad.

Tomando en cuenta lo anterior descrito se hace necesario que los equipos Blue Team de las organizaciones trabajen muy de la mano con el CIS ya que esto le va a permitir estar actualizado y a la vanguardia sobre temas de ciberseguridad, van a poder recibir consejos y verificar si los mismos pueden aplicarse a su entidad, teniendo en cuenta que es una organización internacional, esto va a permitir que los equipos estén mejor preparados y más actualizados, de igual forma pueden recibir acompañamiento para poder implementar las políticas de ciberseguridad que mejor se ajusten a las necesidades de la organización y algo muy importante, como es una organización sin ánimo de lucro, dicho apoyo, asesoría y acompañamiento sería totalmente gratuito.

5.6 SIEM Y XRD

Ilustración 55. Comparativa SIEM Vs XRD

SIEM	XDR	ASPECTO A ANALIZAR
Ofrece capacidades de análisis y gestión de registros centralizados para una entidad.	Se centra en utilizar los datos recopilados para optimizar la detección y respuesta a amenazas.	**Objetivo**
Requiere un esfuerzo de gestión para conectarlas a fuentes de datos y ajustar sus alertas.	Están diseñadas para integrarse con la arquitectura de seguridad de una entidad y proporcionar alertas útiles.	**Gestión**
Es una herramienta de análisis de datos que proporciona los datos y las alertas necesarias para detectar e identificar potenciales amenazas a las que pueda estar expuesta una entidad.	Las soluciones de seguridad brindadas por XDR, amplía la capacidad de respaldar y coordinar los esfuerzos de respuesta dentro de la misma solución, por lo que se puede deducir que plantea una solución integral y holística.	**Respuesta a Incidentes**
Permite el almacenamiento centralizado de datos a largo plazo	Genera un almacenamiento temporal, el tiempo suficiente para el análisis de los datos	**Almacenamiento de Datos**
Ideal para empresas grandes	Es ideal para empresas de pequeño y mediano tamaño	**Uso**
Su implementación es menos compleja	Requiere un conocimiento especializado por parte del personal que brinda solución	**Conocimiento**

Fuente. Autor.

5.7 HERRAMIENTAS DETECCIÓN DE ATAQUES

5.7.1 OSSEC

Ilustración 56. Logo OSSEC

Fuente: https://conocimientolibre.mx/ossec/

Es una herramienta gratuita de detección que intrusos que realiza análisis de registro, detección de rootkits, comprueba la integridad en los registros de Windows, básicamente esta herramienta permite realizar un seguimiento profundo y un análisis detallado sobre las actividades en un servidor.

Principales funciones:

- Respuesta permanente a brechas e incidentes
- Detecta intrusos basado en los registros y comportamientos de un servidor.
- Detección de rootkits
- Monitorea la integridad de archivos.

5.7.2 SURICATA

Ilustración 57. Logo Suricata

Fuente: https://blog.elhacker.net/2021/03/suricata-ids-ips-instalacion-configuracion-reglas-.html

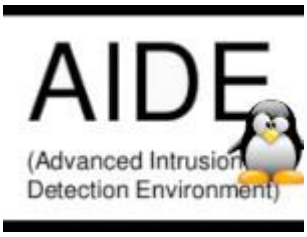
Esta herramienta gratuita es un sistema que permite detectar intrusos, es una herramienta muy robusta y puede realizar dicha detección en tiempo real, así

mismo posibilita prevenir intrusiones en línea y realizar un monitoreo de la red.

Esta herramienta puede actuar tanto en modo pasivo como activo, en el modo pasivo detecta y almacena información sobre el tráfico y comportamiento de la red, y el modo activo, previene intrusiones.

5.7.3 AIDE (ADVANCED INTRUSION DETECTION ENVIRONMENT)

Ilustración 58. AIDE



Fuente:https://www.pc-freak.net/blog/install-configure-aide-advanced-intrusion-detection-environment-debian-gnu-linux-11-monitor-files/

Esta es una utilidad o herramienta de detección de intrusiones, basada en Host y que permite comprobar la integridad de los archivos y así poder detectar intrusiones en el sistema.

Esta herramienta es muy robusta y poderosa y permite monitorear cambios en sistemas Linux o Unix.

6. BLUE TEAM, RED TEAM Y PURPLE TEAM

Una integración de estos tres (3) equipos de seguridad da la posibilidad a la organización de poder estar cada vez más preparada y mejor protegida ante un ataque real de ciberseguridad, ya que como se ha podido conocer e identificar dentro del desarrollo de este curso, los Red Team se encargan de realizar pruebas de penetración en un ambiente controlado, con el fin de evaluar la respuesta, la contención y/o protección de la organización por parte de los Blue Team, generando por cada uno de estos equipos al finalizar dicha prueba presenta un informe en donde se plasman los hallazgos realizados durante el proceso.

Sin embargo, por mucho tiempo el desarrollo de estas labores y procesos se percibían como islas separadas, en donde cada equipo se encargaba de realizar lo de su competencia y en donde muchas veces no había complementariedad por parte de estos equipos, lo que limitaba un mayor aprovechamiento de sus habilidades o imposibilitaba una mejor respuesta por parte de la organización.

Es aquí en donde surge el concepto de purple team y se desarrolla dicho equipo, el cual tiene como función principal el análisis de los informes entregados por los equipos blue team y red team y poder establecer una complementariedad permitiendo que estos equipos se potencialicen el uno al otro, se documenten y se organicen para que el desempeño de sus funciones sean cada vez más eficientes, eficaces y más cercanas a la realidad, posibilitando una mejor y mayor respuesta por parte de la organización ante posibles ataques cibernéticos reales.

7. RECOMENDACIONES

Con el fin de poder mejorar los aspectos de seguridad dentro de una organización, los equipos red team y blue team se pueden aportar al desarrollar una serie de una serie de planes que permiten la reducción de las brechas de seguridad.

7.1 PLAN DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

Este tipo de planes tiene como finalidad establecer un análisis de brechas para poder determinar y/o identificar el nivel de madurez de un SGSI[7] dentro de la organización tomando como lineamiento la norma NTC ISO/IEC 27001:2022[8], así mismo como las acciones a desarrollar para la reducción de dichas brechas.

Con este Plan de seguridad digital, se busca identificar e implementar acciones de mejora que estén enfocadas a fortalecer el aseguramiento de los activos de información dentro de una organización, garantizando con esto la robustez en la prestación de los servicios de la misma y así poder preservar la integridad, disponibilidad y sobretodo la confidencialidad de la información todo esto dentro del marco legal de la Ley 1581 de 2012.

7.2 PLAN DE TRATAMIENTO DE RIESGOS

Este plan tiene como finalidad minimizar el nivel de exposición de organización en amenazas cibernéticas y que a través de la aplicación de los planes de control se pueda preservar la disponibilidad, integridad y confidencialidad de la información dentro de la empresa.

El plan de tratamiento de riesgos reduce la posibilidad que se puedan materializar los incidentes de seguridad la información en la infraestructura TI de la organización, toda a través de los hallazgos que se hayan identificado por parte de los blue team y red team.

---

[7] SGSI – Sistema de Gestión y Seguridad de la Información. ISO 27001. (Septiembre 24 de 2023). Disponible: https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases

[8] NTC ISO/IEC 27001:2022. ICONTEC. (Septiembre 24 de 2023). Disponible: https://tienda.icontec.org/gp-ntc-iso-iec-seguridad-de-la-informacion-ciberseguridad-y-proteccion-de-la-privacidad-sistemas-de-gestion-de-seguridad-de-la-informacion-requisitos-ntc-iso-iec27001-2022.html

7.3 PLAN DE TRATAMIENTO DE DATOS PERSONALES

Este plan tiene como finalidad darle un buen uso a los datos personales que la organización posee tanto de sus clientes, como de sus empleados y/o proveedores, dentro del mismo se contempla el ciclo de vida de los datos personales.

8. VIDEO SUSTENTACIÓN

Parte 1: https://youtu.be/CxwGI4FsEOo

Parte 2: https://youtu.be/VuKhQdjO45A

CONCLUSIONES

El desarrollo de las diferentes actividades nos ha brindado la posibilidad de conocer los diferentes aspectos legales a los que están sujetos los equipos Red Team y Blue Team, así mismo como las sanciones o condenas a las que están expuestas aquellas personas que deseen cometer fraudes y/o delitos informáticos.

Es necesario que como profesionales en el área de TI, tengamos claro y presente el código de ética que no rige, esto con el fin de poder desarrollar y desempeñar nuestra labor de la manera más integra posible.

Así mismo, a través de un buen análisis de riesgo informático en una organización se pueden implementar diferentes metodologías, técnicas y herramientas que le permitan identificar vulnerabilidades en los sistemas informáticos de las organizaciones y a través de esto, prevenir y/o evitar que las vulnerabilidades puedan ser explotadas y así reducir las brechas de seguridad que pueda tener la organización, de igual forma se están protegiendo los activos críticos de la empresa, así como los datos e información de la misma.

A través de una respuesta oportunidad ante un ataque de ciberseguridad, estamos mitigando el impacto que este puede ocasionar o generarle a la organización, ya que se corre el riesgo de que dicho impacto no sea solo económico sino también reputacional.

Es por lo anterior que se hace necesario poder contar con un buen equipo de penetración y contención (Red Team y Blue Team) dentro de la organización, esto con el fin de poder sacar el mayor provecho de las diferentes pruebas de pentesting que se realicen para así poder estar más preparados ante un posible ataque, poder desarrollar planes y políticas de contención y mitigación y de igual forma tener la capacidad de dar respuestas eficaz y oportunidad ante un posible ataque cibernético.

BIBLIOGRAFÍA

LAS FASES DE UN TEST DE PENETRACIÓN (PENTEST). Cyberseguridad.net. [En Línea]. [Consultado: agosto 12 de 2023]. Disponible en: https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i

¿QUÉ ES FOOTPRINTING? Peña, María José [En Línea]. [Consultado: agosto 12 de 2023]. Disponible en: https://eiposgrados.com/blog-ciberseguridad/que-es-footprinting/

HACKING ÉTICO: GUIA COMPLETA DE FOOTPRINTING. Tokio. [En línea]. [Consultado: agosto 13 de 2023]. Disponible en: https://www.tokioschool.com/noticias/footprinting/

HERRAMIENTAS DE HACKING PARA UN HACKING ÉTICO. Esic. [En línea]. [Consultado: agosto 13 de 2023]. Disponible en: https://www.esic.edu/rethink/tecnologia/herramientas-de-hacking-para-un-hacking-etico#:~:text=Primera%20fase%3A%20Footprinting&text=En%20esta%20fase%20son%20%C3%BAtiles,OSINT)%20como%20osrframework%20o%20Maltego.

CiberseguridadTips. Importancia de la Ciberseguridad en las Empresas. [En línea]. [Consultado: agosto 13 de 2023]. Disponible en: https://ciberseguridadtips.com/que-hace-una-empresa-de-ciberseguridad/

LEY 1273 DE 2009. Superintendencia de Industria y Comercio. [En Línea]. [Consultado: agosto 17 de 2023]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

RANSOMHOUSE INFORMACIÓN ROBADA A KERALTY-SANITAS. Muchohacker.lol. [En Línea]. [Consultado: agosto 17 de 2023]. Disponible en: https://muchohacker.lol/tag/keralty/

POST EXPLOTACIÓN CON METERPRETER. Linux-Console.net. [En Línea]. [Consultado: septiembre 01 de 2023]. Disponible en: https://es.linux-console.net/?p=16740#gsc.tab=0

TEST DE INTRUSIÓN Y EXPLOTACIÓN DE VULNERABILIDADES. Universidad de Vigo. [En Línea]. [Consultado: septiembre 01 de 2023]. Disponible en: https://ccia.esei.uvigo.es/docencia/SSI/1819/practicas/ejercicio-metasploit/

COMANDOS DE METERPRETER EN KALI LINUX. CREADPAG. [En Línea]. [Consultado: septiembre 01 de 2023]. Disponible en: https://www.creadpag.com/2018/05/comandos-de-meterpreter-en-kali-linux.html

METASPLOIT. Hack By Security. [En Línea]. [Consultado: septiembre 01 de 2023]. Disponible en: https://www.hackbysecurity.com/blog/metasploit-cheat-sheet-1

Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. Incibe.es. [En Línea]. [Consultado: septiembre 16 de 2023]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

TIPS TECNOLÓGICOS, DE CONFIGURACIÓN Y NEGOCIO QUE COMPLEMENTAN TU SEGURIDAD. Blog Smartekh. [En Línea]. [Consultado: septiembre 16 de 2023]. Disponible en: https://blog.smartekh.com/que-es-hardening

10 ETAPAS DE HARDENING DE WINDOWS PARA MEJORAR LA RESILIENCIA CIBERNÉTICA. CalCom. [En Línea]. [Consultado: septiembre 16 de 2023]. Disponible en: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

¿Qué es el centro para la seguridad de Internet (CIS)?. Krypton SOLID. [En Línea]. [Consultado: septiembre 17 de 2023]. Disponible en: https://kryptonsolid.com/que-es-el-centro-para-la-seguridad-de-internet-cis/

GUÍA COMPLETA SOBRE CONTROLES DE SEGURIDAD CIS. Ciberseguridad.com. [En Línea]. [Consultado: septiembre 17 de 2023]. Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/

¿Qué es OSSEC?. KEEPCODING Tech School. [En Línea]. [Consultado: septiembre 17 de 2023]. Disponible en: https://keepcoding.io/blog/que-es-ossec/

¿Qué es Suricata en Ciberseguridad?. KEEPCODING Tech School. [En Línea]. [Consultado: septiembre 17 de 2023]. Disponible en: https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

AIDE (Español). archlinux. [En Línea]. [Consultado: septiembre 19 de 2023]. Disponible en: https://wiki.archlinux.org/title/AIDE_(Espa%C3%B1ol)

Las 8 mejores herramientas open source de detección de intrusión. OpenWebinars. [En Línea]. [Consultado: septiembre 19 de 2023]. Disponible en: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

CSIRT. SECUREIT. [En Línea]. [Consultado: septiembre 19 de 2023]. Disponible en: https://www.secureit.es/csirt/

Red Team, Blue Team y Purple Team, ¿Cuáles son sus funciones y diferencias?. Unir. [En Línea]. [Consultado: septiembre 19 de 2023]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

¿COMO DETECTAR UN CIBERATAQUE DE FORMA RÁPIDA PARA PROTEGER TU NEGOCIO?. WSECURITY.ONLINE. [En Línea]. [Consultado: septiembre 19 de 2023]. Disponible en: https://www.wsecurity.online/blog/como-detectar-ciberataque