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

JUAN CARLOS CERCADO GUERRERO

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

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

JUAN CARLOS CERCADO GUERRERO

DIRECTOR DE CURSO

LUIS FERNANDO ZAMBRANO

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

CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

En este informe se destaca la importancia crítica de fortalecer las estrategias en los equipos de Blue y Red Team. Para ello, se analizarán las principales características y responsabilidades de cada equipo, se presentarán ejemplos concretos de su aplicación en la práctica y se formularán recomendaciones específicas para mejorar los procesos y la seguridad de la información.

Palabras claves: **Ataque, Ciberseguridad, Pentesting, Team, Vulnerabilidad**

ABSTRACT

This report highlights the critical importance of strengthening strategies in Blue and Red Teams. To do this, the main characteristics and responsibilities of each team will be analyzed, concrete examples of their application in practice will be presented, and specific recommendations will be formulated to improve processes and information security.

Keywords: Attack, Cybersecurity, Pentesting, Team, Vulnerability

GLOSARIO

Ciberseguridad: Tejido invisible que protege la información digital.

Vulnerabilidad: Huella digital que deja una puerta entreabierta.

Ataque: Asedio virtual para conquistar información o causar daño.

Equipo Red Team: Simula ataques para mejorar seguridad.

Equipo Blue Team: Defiende contra ataques cibernéticos.

Explotación sexual infantil: Beneficio sexual a cambio de dinero, bienes o servicios

Cibercrimen: Delito usando tecnologías de la información.

Payload: Carga útil que se ejecuta en el sistema objetivo para obtener acceso o control.

Pentesting: Pruebas de penetración para identificar vulnerabilidades en un sistema.

Nmap: Herramienta para mapear redes y escanear puertos abiertos

Phishing: Suplantación de identidad para engañar a la víctima y obtener información confidencial.

Purple Team: Equipo que combina las habilidades de los equipos Red Team y Blue Team.

INTRODUCCIÓN

El presente informe técnico tiene como objetivo principal abordar los conceptos básicos en el contexto de los equipos de Blue Team y Red Team, teniendo en cuenta los criterios legales y normatividad vigente. Se busca analizar la complejidad de las aplicaciones y las deficiencias en las prácticas de estos equipos, con el fin de proponer estrategias para fortalecer su eficacia en la protección de la información.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Fortalecer las estrategias de los equipos de Blue Team y Red Team para mejorar la seguridad de la información.

1.2 OBJETIVOS ESPECIFICOS

- Examinar las fallas y deficiencias en los sistemas de cómputo.
- Evaluar la capacidad de respuesta y reacción del equipo de Blue Team frente a vulnerabilidades conocidas y actualizaciones de seguridad.
- Formular estrategias concretas para fortalecer los procesos de seguridad.

2 DESARROLLO DEL INFORME

3 ESCENARIO 1

3.1. MARCO REGULATORIO COLOMBIANO SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES: ANÁLISIS DE LAS LEYES 1273 DE 2009 Y 1581 DE 2012.

La Ley 1273 de 2009, plantea por primera vez de manera explícita la adecuación típica de Delitos Informáticos y protección del bien jurídico tutelado que es “de la protección de la información y de los datos” (Congreso de la República de Colombia, 2009) sin embargo, no regula mecanismos de protección al consumidor de productos financieros. Algo semejante ocurre, con la entrada en vigor de la Ley 1341 de 2009 “por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro” (Congreso de la república, 2009). Esta última constituye un referente, en materia de protección a los usuarios del espectro electromagnético y en particular para los usuarios del ciberespacio y en las acciones y actos de comercio enmarcadas en el ciberespacio.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que

utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". [1]

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de estos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo.

En lo que corresponde a la legislación colombiana, puede reconocerse con ocasión de la expedición de la Ley 1273 de 2009,) existe un punto de inflexión sobre el tratamiento punitivo del asunto en cuestión, ya que es por la misma, que se modifica el Código Penal Colombiano, Ley 599 de 2000, creando un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos" y se toman medidas concernientes a la protección integral de los sistemas que usan TIC.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado «De la Protección de la información y de los datos» que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

[1] LEYES DESDE 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009] [Anónimo]. SECRETARÍA GENERAL DEL SENADO [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

En el que se consigna como delitos; el acceso abusivo a un sistema informático; la obstaculización ilegítima de sistema informático o red de telecomunicación; la interceptación de datos informáticos; el daño informático; el uso de software malicioso; la violación de datos personales; y la suplantación de sitios web para capturar datos personales. El Congreso de Colombia decreta la adición al Código Penal del título VII bis, “De la protección de la información y de los datos”, el cual se compone únicamente de dos capítulos, a saber: El delito informático con mayor pena de prisión en Colombia es el hurto por medios informáticos y semejantes, el cual consiste en superar medidas de seguridad informáticas para apoderarse de una cosa mueble ajena, con el fin de obtener provecho para sí o para otro, mediante la manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante o mediante la suplantación de un usuario ante sistemas de autenticación y de autorización establecidos (Congreso de la República de Colombia, 2009).

3.2. ANÁLISIS DETALLADO DE LA ETAPA DE FOOTPRINTING EN PENTESTING: HERRAMIENTAS Y SIGNIFICADO EN CIBERSEGURIDAD.

Término empleado en ciberseguridad para referirse a la recolección de información de un sistema, susceptible de ser empleada en un ciberataque. Dicha información se suele encontrar disponible generalmente en canales de acceso público, como buscadores de Internet. El footprint es el rastro dejado por el concepto que se pretende investigar y que define en mayor o menor medida un sistema, red o empresa[2].

Las metodologías de intrusión y Testing son los procedimientos, prácticas y técnicas que se utilizan para evaluar el estado de conformidad de la

[2] GLOSARIO de Ciberseguridad | MNEMO [Anónimo]. MNEMO | Ciberseguridad, Transformación Digital [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://mnemo.com/glosario-ciberseguridad/

infraestructura tecnológica a nivel de seguridad, simulando un ataque real por parte de un hacker malicioso. El objetivo es identificar y explotar las vulnerabilidades que puedan comprometer la integridad, confidencialidad o disponibilidad de la información o los recursos. Existen diferentes tipos y metodologías de intrusión y Testing, según el grado de conocimiento previo, el origen del ataque, el alcance y la profundidad del análisis

Encontrará vulnerabilidades dentro de un entorno de objeto definido:

- Se aplicar pruebas de penetración centradas en la seguridad de un área específica definida para las pruebas.
- Se tienen conocimiento de metodologías especificas en pentesting
- Es preciso en identificar “como” y “cuando” ejecutarlas por cada tecnología.

Las considero importantes toda vez que con un enfoque ético de pruebas de seguridad donde profesionales autorizados simulan ataques para identificar vulnerabilidades. El objetivo es mejorar la seguridad al descubrir y corregir debilidades antes de que puedan ser explotadas de manera malintencionada.

3.3. EXPLORACIÓN DE METASPLOIT Y USO DE CVES EN LA CIBERSEGURIDAD.

Una vulnerabilidad de seguridad se puede ver como el punto de partida de todo el proceso que implica la seguridad en general.

Una vulnerabilidad permite, de alguna manera, a los atacantes alterar el comportamiento normal de un programa.

Una vulnerabilidad está definida:

1. Producto >>> aplicación, dispositivo, sistema de información, o sistema de comunicación afectado.

2. Donde >>>> que componente es afectado por la presencia de la vulnerabilidad.

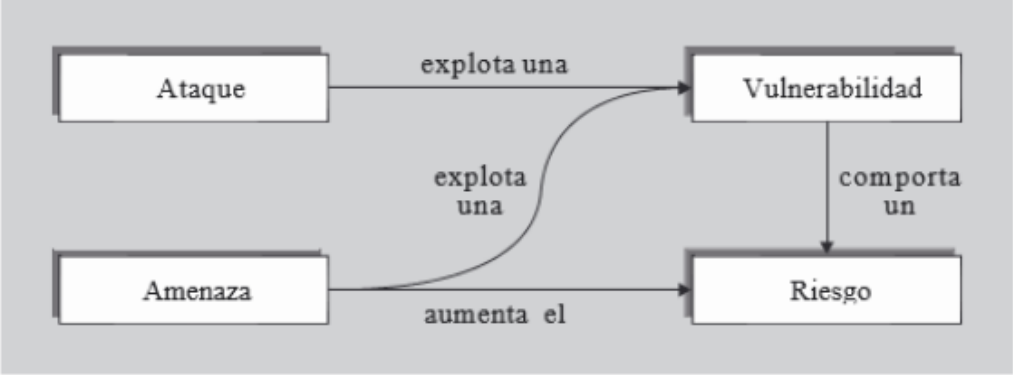
3. Causa >>>> el fallo técnico concreto (DoS, Hombre en medio, perdida de tramas, instalación de un código malicioso……).

4. Impacto >>>> el gravo de gravedad (leves, medio, alto, critica).

5. Vector >>> Técnica de ataque (ataque pasivo, activo, intrusión en la red, intercepción en el intercambio de manos).

Los conceptos de seguridad en Sistemas de información nacen de la adecuada definición de ataques, amenazas y riesgos a los que puede dar lugar una vulnerabilidad[3].

Figura 1 El ciclo de la vulnerabilidad: De la amenaza al riesgo



Fuente: https://es.slideshare.net/moplin/gestin-de-vulnerabilidades

Las vulnerabilidades están siendo estudiadas por los delincuentes y los expertos para atacar un sistema y para proteger un sistema, para ello hay diferentes formas de recopilar, catalogar y publicar una vulnerabilidad.

[3] ¿QUÉ ES una vulnerabilidad en seguridad informática? Ejemplos [Anónimo]. Blog HostDime Perú, Servidores dedicados [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/

Figura 2 CVE: El lenguaje universal de las vulnerabilidades

Fuente: https://www.abbr.com/images/79778_CVE.png

Figura 3 Ciclo de vida de una vulnerabilidad.

Fuente: Elaboración propia.

CVSS distingue entre tres métricas básicas.

Métrica base, esta mide aspectos de la vulnerabilidad constantes en el tiempo y entorno en que se puede dar la explotación de esta, estas métricas proporcionan un valor que se expresa como vector:

AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C].

Actualmente se definen dos variantes de métrica V2.0 y V3.0, esta es un ejemplo de CVE 2.0; la vulnerabilidad CVE-2002-0392 tiene el siguiente vector base:

AV:N/AC:L/Au:N/C:N/I:N/A:C

Figura 4 Descripción del Vector.

Vector de acceso (AV)	Cómo se explota la vulnerabilidad. Puede ser localmente (L), desde una red adyacente (A) o desde cualquier red (N).
Complejidad de acceso (AC)	Complejidad que requiere el atacante una vez ha accedido al sistema. Esta puede ser alta (H), media (M) o baja (L).
Autenticación (Au)	Número de veces que el atacante debe autenticarse contra un sistema. Pueden ser múltiples (M), una (S) o ninguna (N).
Impacto de confidencialidad (C)	Tres indicadores sobre el impacto que puede tener la vulnerabilidad en estos tres pilares de la S. Información del sistema. Para cada uno los valores puede ser: ninguno (N), parcial (P) o completo (C).
Impacto de integridad (I)	
Impacto de disponibilidad (A)	

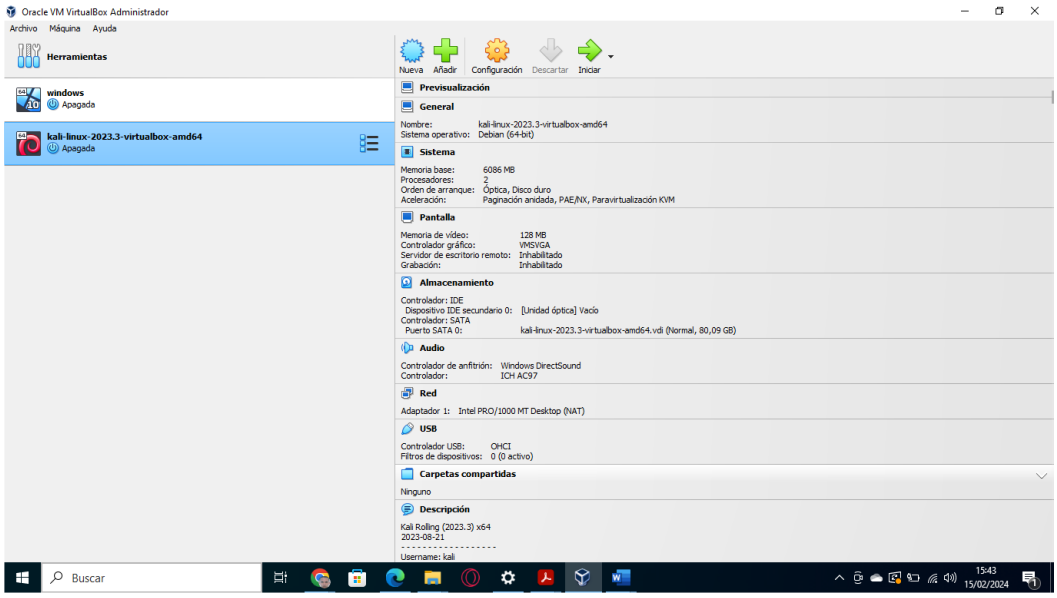
Fuente: Elaboración propia.

Figura 5 Herramientas.

Fuente: https://fferia.wordpress.com/nessus/

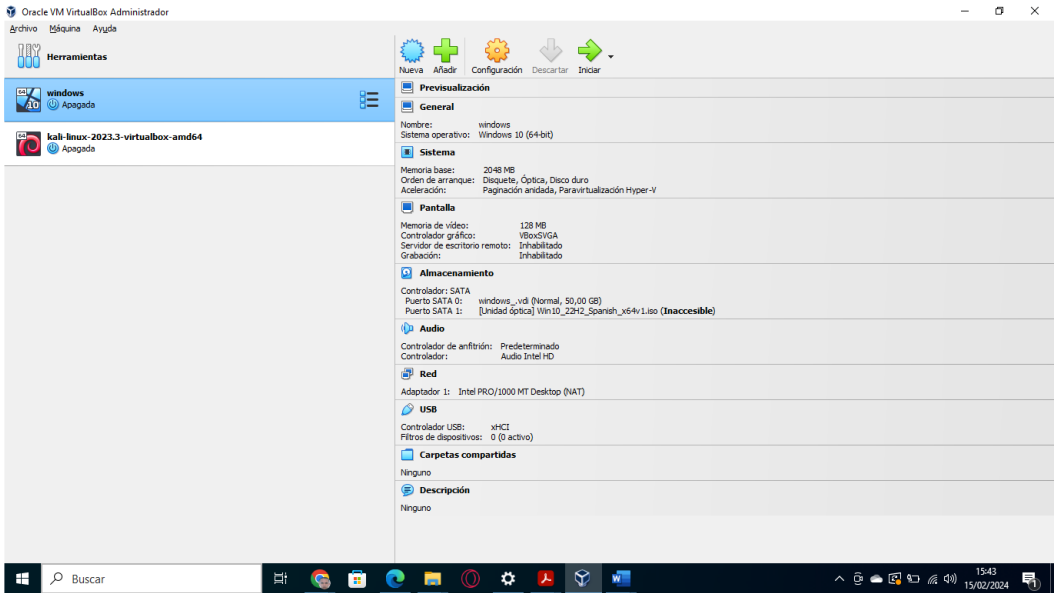
3.4. CONFIGURACIÓN Y ANÁLISIS DE ESCENARIO: BANCO DE TRABAJO PARA ACTIVIDADES DE ALTA TECNICIDAD.

Figura 6 Ambiente de trabajo



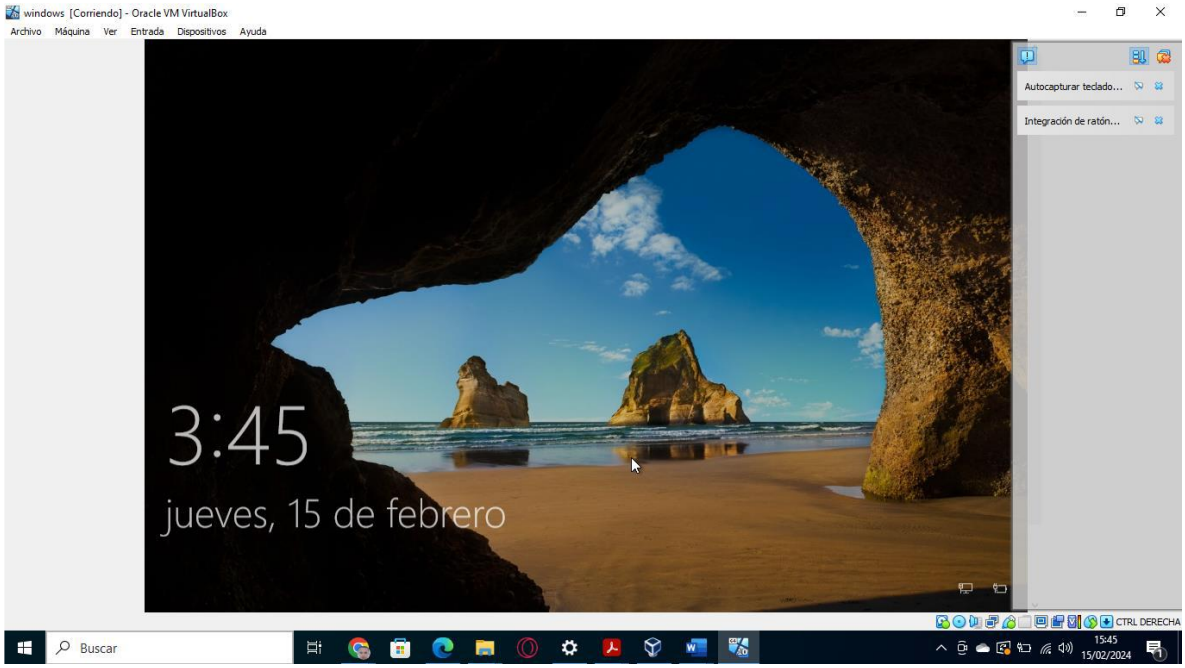
Fuente: Elaboración propia.

Figura 7 Configuración máquinas virtuales



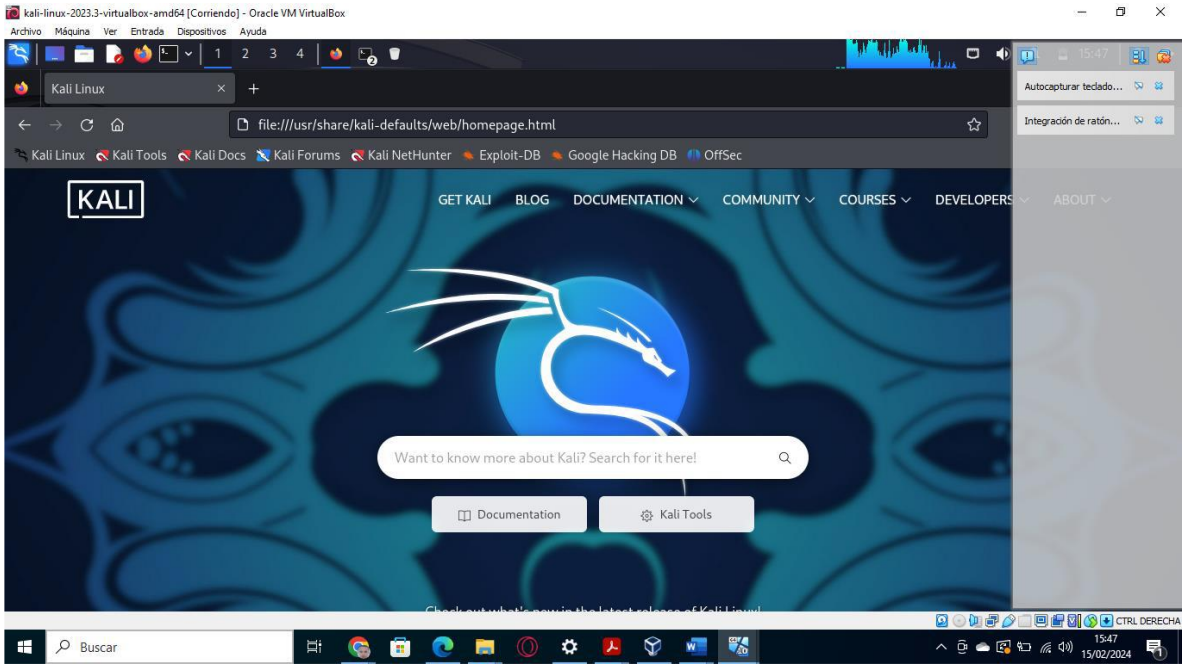
Fuente: Elaboración propia.

Figura 8 Maquina Windows



Fuente: Elaboración propia.

Figura 9 Maquina LINUX



Fuente: Elaboración propia.

4 ESCENARIO 2

4.1. ¿QUÉ PÁRRAFOS CREE USTED QUE SE TORNAN ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD?

La Constitución de 1991 se encuentra enmarcada en la filosofía de la subordinación de la ley a los valores y principios que fueron convalidados por el consenso político (art. 4°), el respeto por la dignidad humana, la igualdad, el debido proceso y demás garantías y derechos ciudadanos, los cuales se constituyen en las guías estatales en procura de sus fines.

El principio de legalidad y la función pública asociada a la sociedad de la información, representa la consolidación de estos en todos los ambientes y nuevos escenarios que otorgan los ambientes virtuales, que a pesar del anonimato propio de la mayoría de los proceso digitales, se procura por mantener los principios constitucionales además que éticos y morales, sobre la información reservada y personal de una persona en sistemas informáticos, redes y bases de datos, a los cueles se les debe brindar la protección en el entorno que vaya migrando en paralelo a las tecnologías.[4]

4.2. PROCESO ILEGAL EN EL ANEXO 3

Constituyendo un referente relevante a la hora de establecer actividades que contrarresten los problemas y desafíos identificados siendo base fundamental para los objetivos establecidos en la presente guía se analiza los siguiente:

La ratificación por parte del Estado Colombiano del Convenio celebrado por Naciones Unidas en Budapest en el año 2019, se consolidó la formulación de una política de Estado dirigida a implementar estrategias para fortalecer los datos personales frente al aumento del cibercrimen tras el auge del consumo virtual de productos financieros.

Una de estas medidas implementadas por el Estado Colombiano, es la criminalización a través de la creación de tipos penales, cuyo contenido específico se dirige a prevenir y castigar las conductas relacionadas con la ciberseguridad. Estos tipos penales se encuentran consignados en el ordenamiento jurídico colombiano en los siguientes apartados del código penal:

- Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se

[4] Corte Constitucional de Colombia | Guardián de la Constitución. [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://www.corteconstitucional.gov.co/inicio/Constitucion-Politica-Colombia-1991.pdf

mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes(Congreso de la República de Colombia, 2000).

- Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses (Congreso de la República de Colombia, 2000).

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor (Congreso de la República de Colombia, 2000)

- 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 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 (Congreso de la República de Colombia, 2000).

Así las cosas, De acuerdo con la opinión de la Red Iberoamericana de Protección de datos, a pesar de los intentos de la legislación colombiana por establecer mecanismos efectivos para garantizar la protección de los usuarios y consumidores virtuales, dada su naturaleza volátil y difusa en la que se enmarca el Cibercrimen, estas medidas resultan insuficientes (Red Iberoamericana de Protección de datos, 2020).

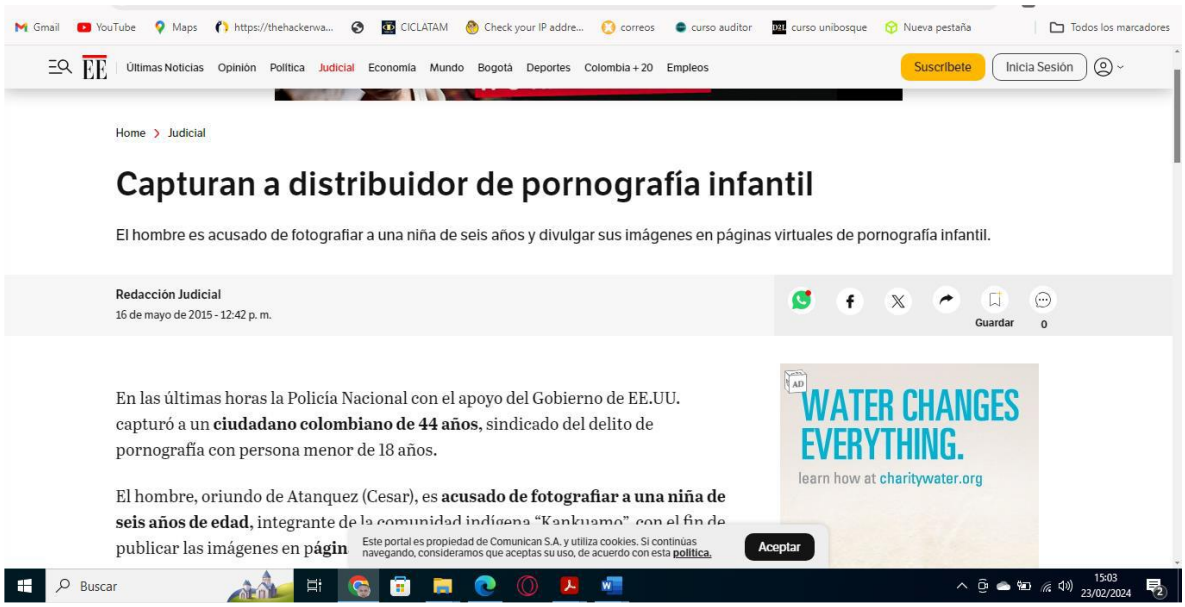
En otras palabras, deben identificarse los principales elementos y modalidades de ejecución del ciberdelito, con el fin de lograr diseñar instrumentos prospectivos que incidan directamente en los niveles de comisión de estos.

4.3. ACEPTAR O NÓ EL CONTRATO EN CASO DE ENCONTRAR PROCESOS ILEGALES EN EL ACUERDO DE CONFIDENCIALIDAD.

El uso de las tecnologías de la información y las telecomunicaciones exige de los que tenemos la oportunidad de ser especialistas en el tema, en relación con las personas y empresas de un entorno donde se maneje información confidencial sensible y privada, se van focalizado en conceptos de transparencia e integridad de los expertos que conllevan cero tolerancia hacia el aprovechamiento indebido de las funciones en cualquiera que sea los cargos y responsabilidades asignadas, el abuso de poder y del conocimiento, y en general, respecto a aquellas conductas que violan los intereses del particular con una excusa de políticas empresariales, al contrario se de procurar por perseguir temas indebidos de carácter particular en los procesos liderados por los todos los sectores y autoridades, donde se hace necesario intervenir para prevenir conflictos de intereses y por supuesto denunciar con el propósito de que se disminuyan están conductas ilegales, NO aceptaría el cargo.

4.4. DECISION FINAL.

Figura 10. Evidencia Articulo Capturan a distribuidor de pornografía infantil.



Fuente:https://www.elespectador.com/judicial/capturan-a-distribuidor-de-pornografia-infantil-article-560937/

Un problema que agobia a la humanidad y afecta en especial a los niños, niñas y adolescentes, quienes son instrumentalizados para la producción de material de abuso sexual infantil y la carencia en la autoridades de Colombia para investigar,

este es un problema global en cual se requieren acciones que permitan mitigar este flagelo desde la prevención y judicialización de los cibercriminales, que cada vez más por el uso del internet y de los programas que se pueden instalar en los computadores y la masificación de las redes sociales que coexisten, permiten mayor campo de acción para cometer los ilícitos y le genera mayor seguridad para no ser descubiertos.

La posibilidad de realizar comportamientos criminales al margen del espacio físico se hace presente con el desarrollo de las nuevas tecnologías, y se crea de este modo una compleja problemática en el ámbito jurisdiccional. En esta línea, para hacer frente a esta nueva ola de comportamientos típicos. Uno de los problemas fundamentales ligados al desarrollo y evolución de las nuevas tecnologías atañe a la necesidad de implementar programas de actuación en la erradicación de todos aquellos delitos relacionados con las redes. En este sentido, son distintos los aspectos objeto de tratamiento; esto es, desde los organismos encargados de intervenir en la lucha contra el crimen, o las políticas de prevención que se deben llevar a cabo, hasta aquellos colectivos de especial vulnerabilidad, los cuales, entiendo, debieran gozar de un tipo de protección especial.

Importante tener en cuenta que una característica importante de los sujetos activos en el cibercrimen es su creciente anonimato, propiciado no solo por las modernas técnicas de encriptación o cifrado, el uso de datos pseudonimizados que permiten separar los mensajes de la identidad del emisor, dificultar el sentido de los mensajes o el empleo de sistemas que entorpecen la trazabilidad de las acciones del atacante en los sistemas vulnerados; sino también, por la enorme dificultad para determinar la relación entre el uso de un equipo informático que se conecta mediante una determinada IP y un criminal. Ello sin contar con la posibilidad de suplantar a un usuario legítimo mediante el uso de software de efectos dañinos cuando se utilizan redes Wifi.

5 ESCENARIO 3

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

En el presente informe de contexto académico se utilizaron las herramientas vistas durante el transcurso de la materia, pero en especial la Máquina VirtualBox versión junto a la herramienta combinado con Nmap y Metasploit Framework, así como Metasploitable2, que en este caso simula la organización para la cual estamos realizando la consulta de Pentesting.

Una vez, contando con los permisos que la organización nos ha concedido, procedemos a intentar ingresar, aprovechando esta vulnerabilidad, obteniendo los resultados esperados para el desarrollo de la actividad.

Una vulnerabilidad de seguridad se puede ver como el punto de partida de todo el proceso que implica la seguridad en general, su presencia puede permitir alterar el comportamiento normal de un programa (realizar algo malicioso como alterar información sensible, interrumpir o destruir una aplicación o tomar su control).

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

Con el propósito de evidenciar una efectiva defensa de los equipos de Blue Team, focalizados en la seguridad defensiva, protegiendo los sistemas y sobre todo los datos, contra los riesgos que representa las diferentes amenazas cibernéticas, monitoreando la red, detección oportuna y generar respuesta efectiva a los incidentes que afecten la política de implantación de una entidad la clasificación de las vulnerabilidades y su respectiva gestión.

Analizando dichos focos se tuvo en cuenta informes estandarizados de las metodologías y las entidades, de las cuales se extrajo, lo ítems, procedimientos y funciones de estos profesionales, con el fin de clasificar y evaluar las taras para individualizar y priorizar las estrategias.

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

Las pruebas de penetración son prácticas, actividades o acciones que se realizan sobre un sistema informático a través de diferentes herramientas, que tienen por objetivo encontrar vulnerabilidades, que puedan hallarse en el mismo.
Cuando una organización acude a estas prácticas son llevadas a cabo por personal idóneo preferiblemente con certificación en ética profesional pues lo que se trata es de acceder a los sistemas de información utilizando diferentes técnicas, que pueden llegar a ser concluyentes.

Dentro del sistema de información se pueden implementar aplicaciones en software que pueden ser programables para que las mismas sean automáticas, que buscan encontrar esas fisuras de seguridad que pueden ser aprovechadas por entes internos o externos.

A esta actividad se le conoce como pentesting que estas compuesto por dos palabras, una es penetración y la otra de test, cuyo objeto es determinar si las políticas de seguridad de la información que buscan la autenticidad, integridad y confidencialidad se conserven dentro de una organización.

Mientras el escaneo de vulnerabilidades está enfocado en la transmisión de datos y la manera en que los mismos pasan por las diferentes capas, aplicado en software y hardware cuyo fin es determinar la existencia de alguna vulnerabilidad y si la misma es interna o externa a la organización, por otra parte, una prueba de penetración puede tener otro tipo de contexto, ya que en la prueba de penetración se observa desde la implementación de las Políticas de Seguridad, confirman su eficiencia, la eficacia, por ende las mismas no son solo en software o hardware, sino que contemplan otras variables que se encuentran contenidas dentro de las políticas de la organización.

Nmap es una herramienta de mapeo de redes. En este caso nos interesa conocer los puertos que se encuentren abiertos, por lo que utilizamos las siguientes flags o argumentos:

- -A : Habilita la detección de SO y de versión, es decir, va a intentar conocer el sistema operativo que está corriendo nuestro objetivo, junto al servicio asignado a cada puerto y su versión.

- -p- : Escanea absolutamente todos los puertos. Por defecto, nmap sólo escanea los puertos más comunes, pero puede que haya otros que contengan información.

Para este ejercicio el puerto 443 es el puerto HTTPS por defecto, este puerto este asociado a las comunicaciones de las redes seguras. Utiliza el protocolo HTTPS, que es la versión segura de HTTP. Para este protocolo se incorpora protocolos de seguridad más fuertes.

El puerto 443 utiliza protocolos TLS para proporcionar una conexión segura entre el cliente y el servidor. De este modo, cualquier dato transmitido a través de este puerto se encripta, lo que garantiza una conexión segura y protege la información de posibles fisgones.

Este puerto es esencial para los sitios web de comercio electrónico y banca en línea, donde se transmiten datos confidenciales como números de tarjetas de crédito y datos bancarios.

El puerto 443 también se utiliza para otros servicios que requieren conexiones seguras, como los servidores de correo electrónico y las VPN. Esta amplia gama de aplicaciones hace del puerto 443 una parte integral de una red segura.

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

Para fortalecer los procesos que contribuya a la reducción de los riesgos, se establecieron instrumentos de recolección de información los cuales, permiten establecer los parámetros esenciales para estructurar de una manera adecuada y acorde a las necesidades, recopilando información como experto en ciberseguridad, para continuar analizando los datos recopilados, después de realizar cuantificación y la decodificación de los instrumentos de recolección de información.

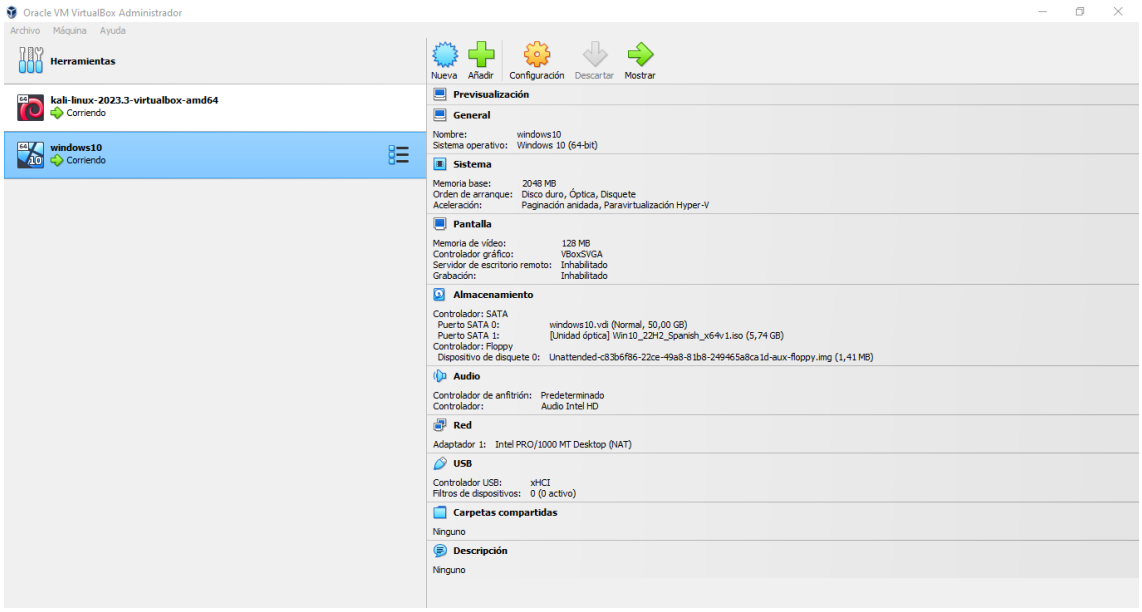
El análisis se focalizándose en sus componentes tecnológicos que permitan las conexiones de los equipos terminales con los servidores y a su vez la trasmisión en tiempo real de la información.

Gestionar las debilidades del sistema, a la entidad siempre estará acompañada de soluciones oportunas que garanticen menor porcentaje de riesgo dedicado a tratar las fragilidades del sistema Windows el cual le fueron desactivados todas las herramientas de protección.

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

Se evidencia la instalación de las maquinas necesarias para el ejercicio:

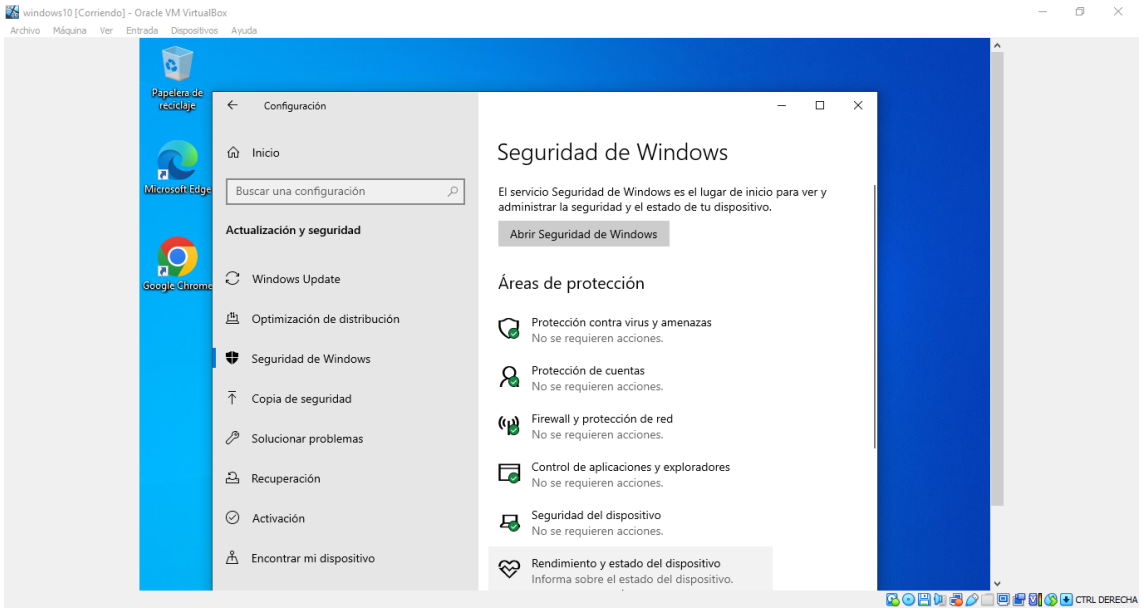
Figura 11 Entorno de trabajo 2



Fuente: Elaboración propia.

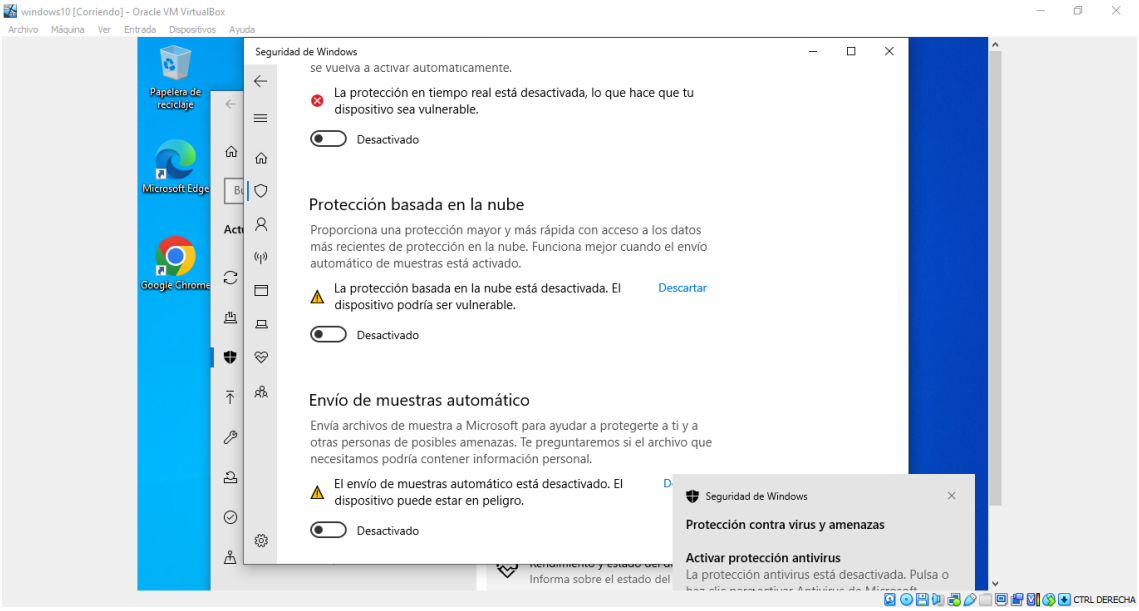
Se videncia la desactivación de la seguridad de la maquina Windows.

Figura 12 Desactivación de la protección



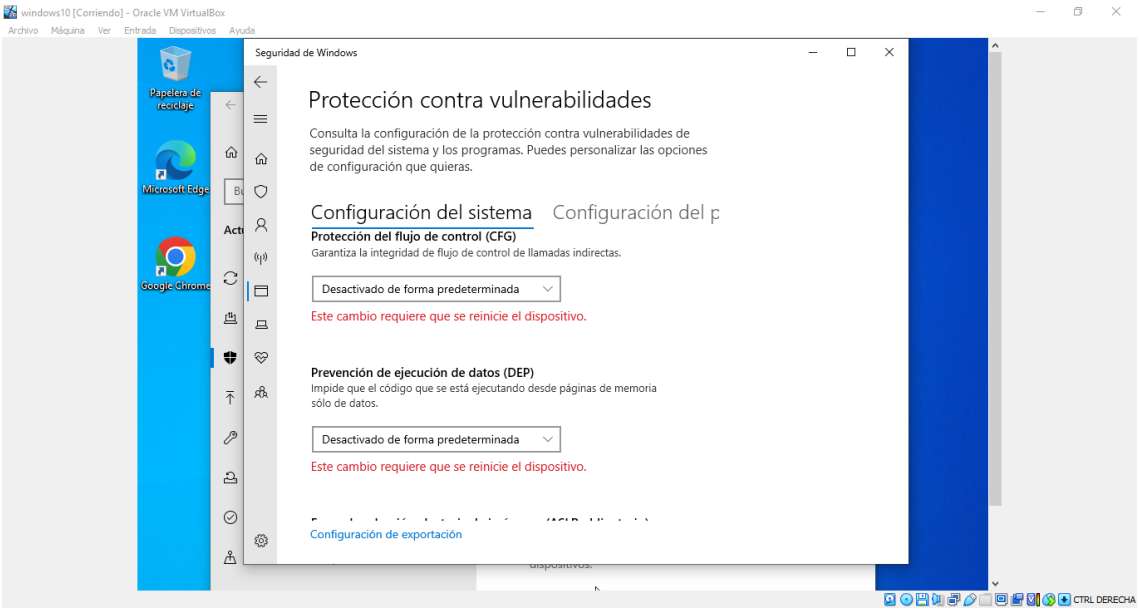
Fuente: Elaboración propia.

Figura 13 Configuración de protección



Fuente: Elaboración propia.

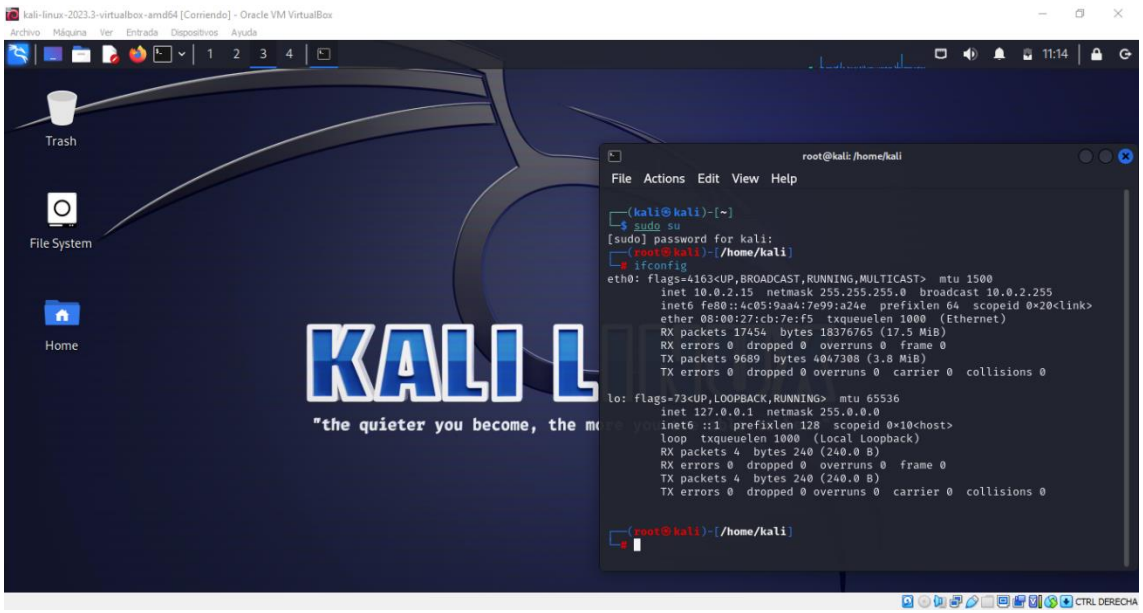
Figura 14 Protección de vulnerabilidades



Fuente: Elaboración propia.

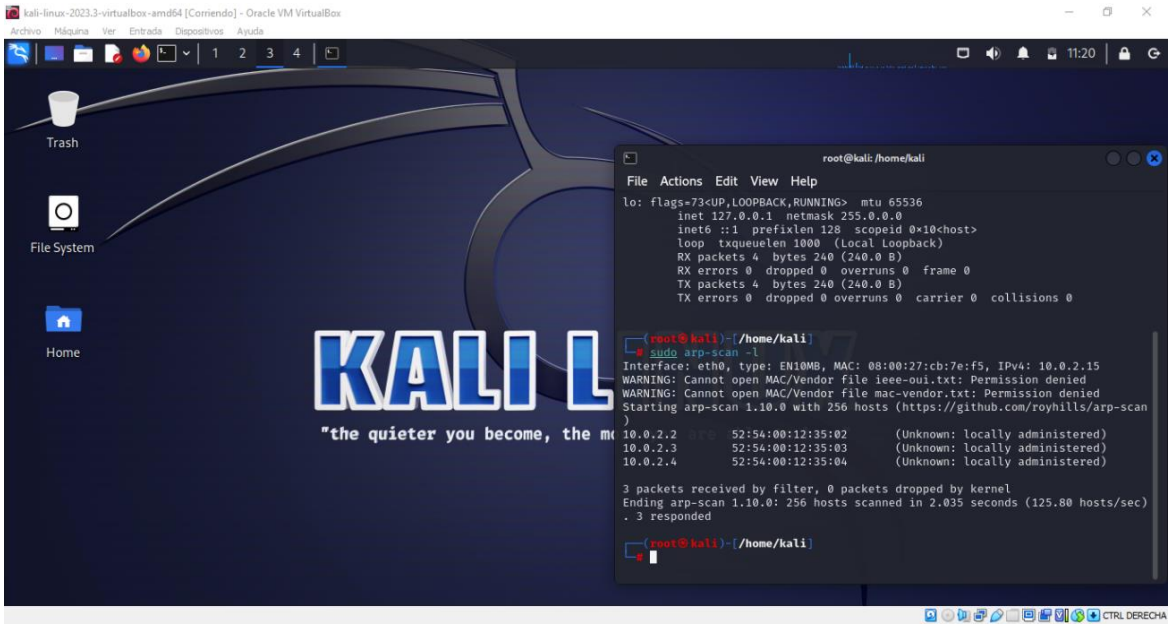
Se evidencia los IP de las maquinas necesarias para el ejercicio de las cuales necesitamos las direcciones IP.

Figura 15 Consulta IP



Fuente: Elaboración propia.

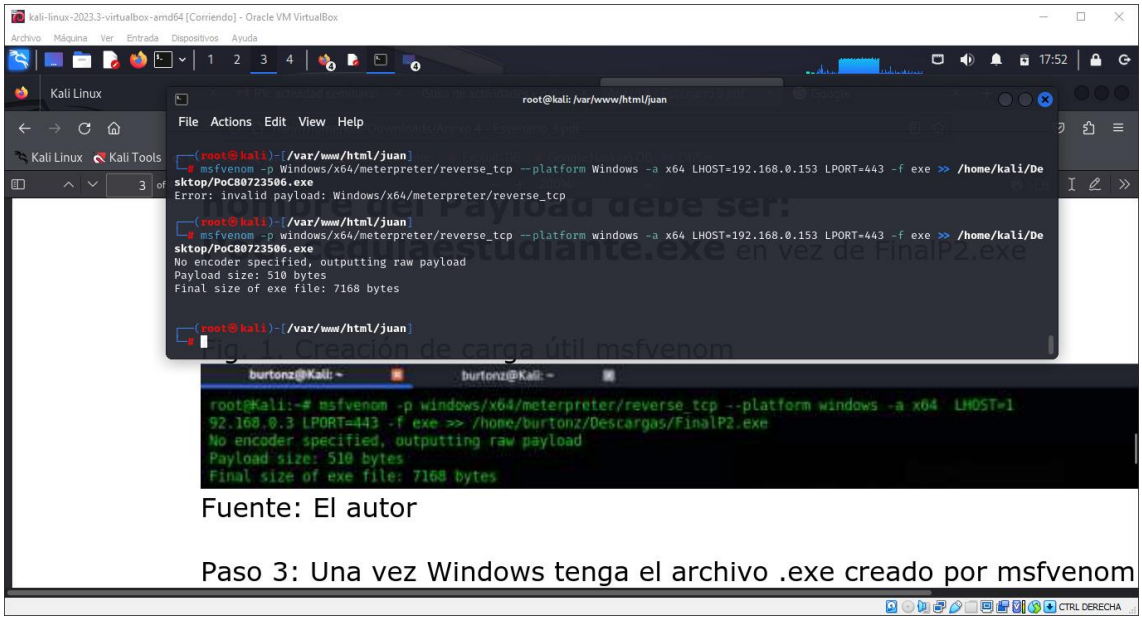
Figura 16 Resultados consultas IP



Fuente: Elaboración propia.

Se evidencia la creación del archivo PAYLOAD, que vamos a ejecutar.

Figura 17 Comandos del archivo



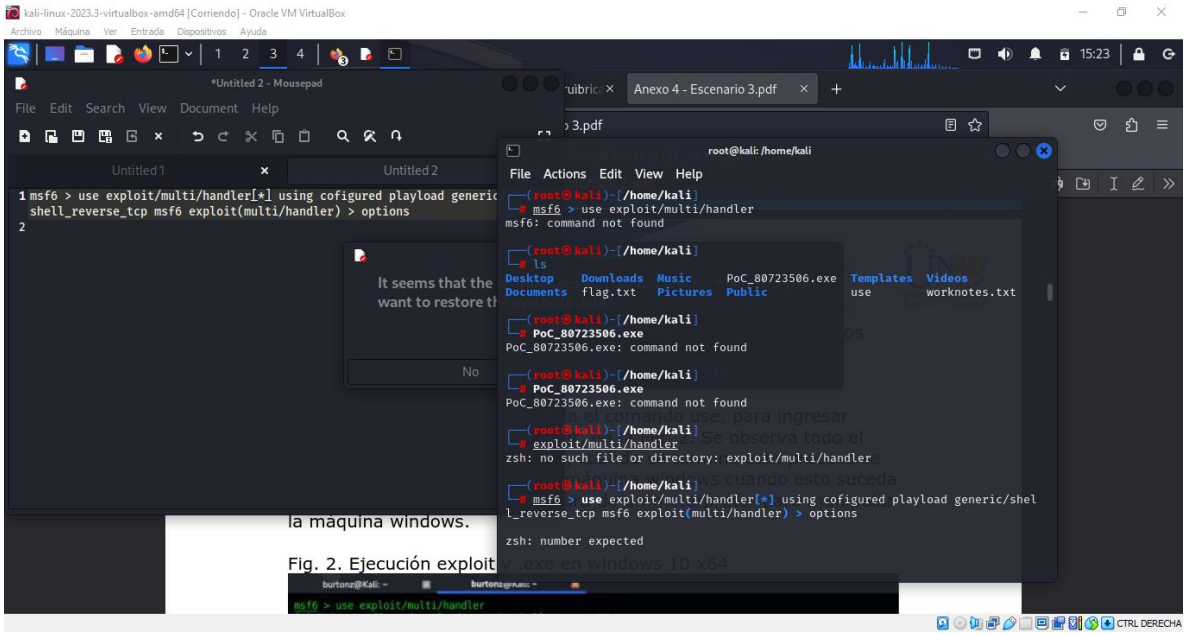
Fuente: El autor

Paso 3: Una vez Windows tenga el archivo .exe creado por msfvenom

Fuente: Elaboración propia.

Se verifica la ruta del archivo que vamos a ejecutar.

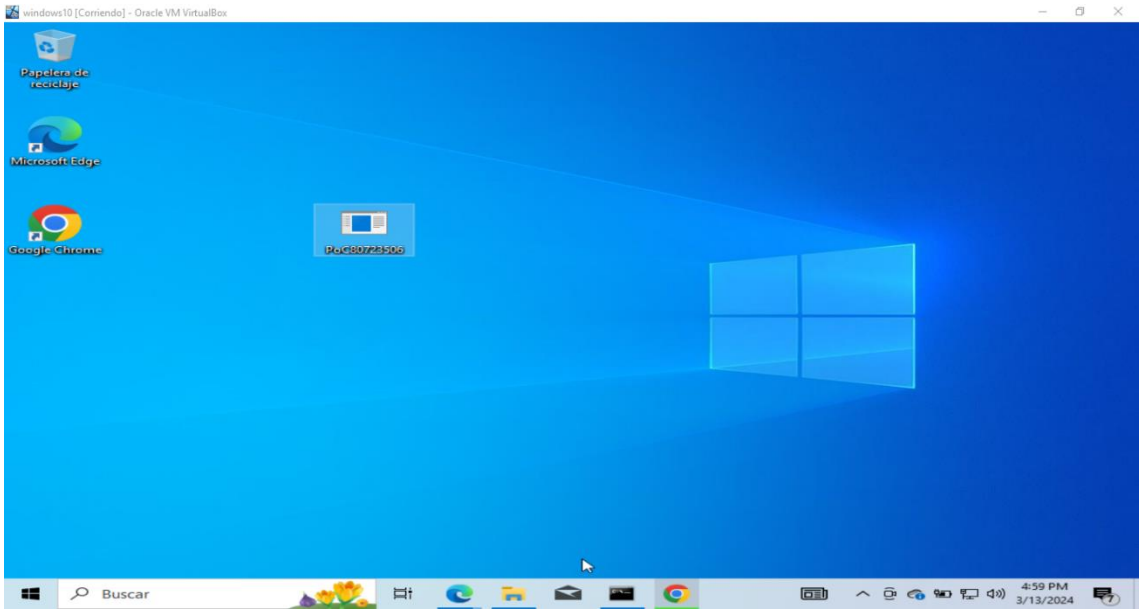
Figura 18 Comandos ruta del archivo



Fuente: Elaboración propia.

Se evidencia la ubicación del archivo en la maquina Windows.

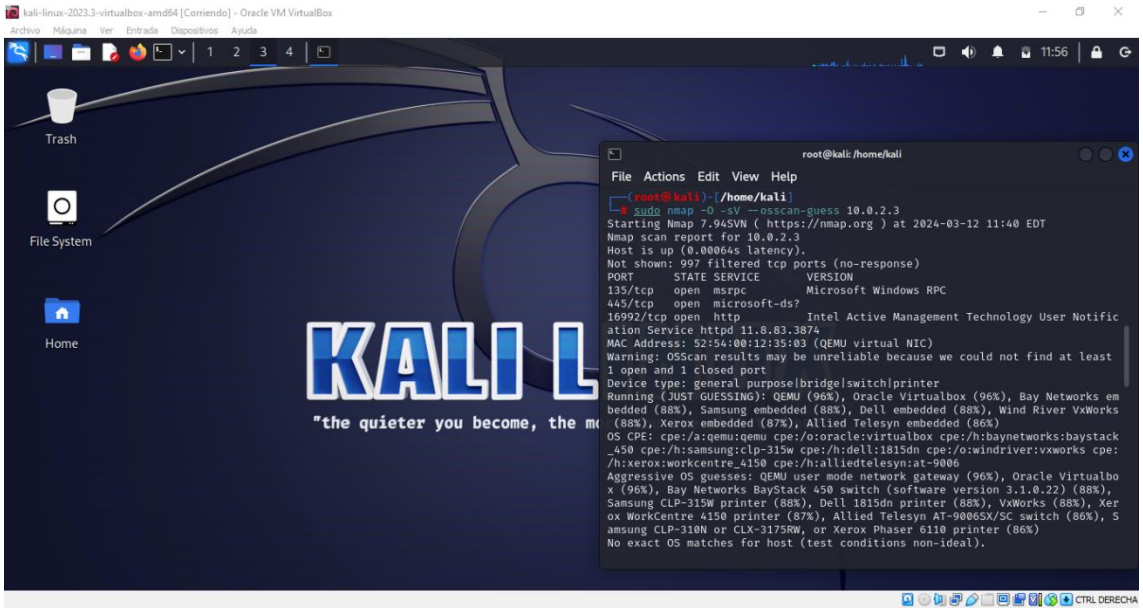
Figura 19 PAYLOAD en la maquina windows



Fuente: Elaboración propia.

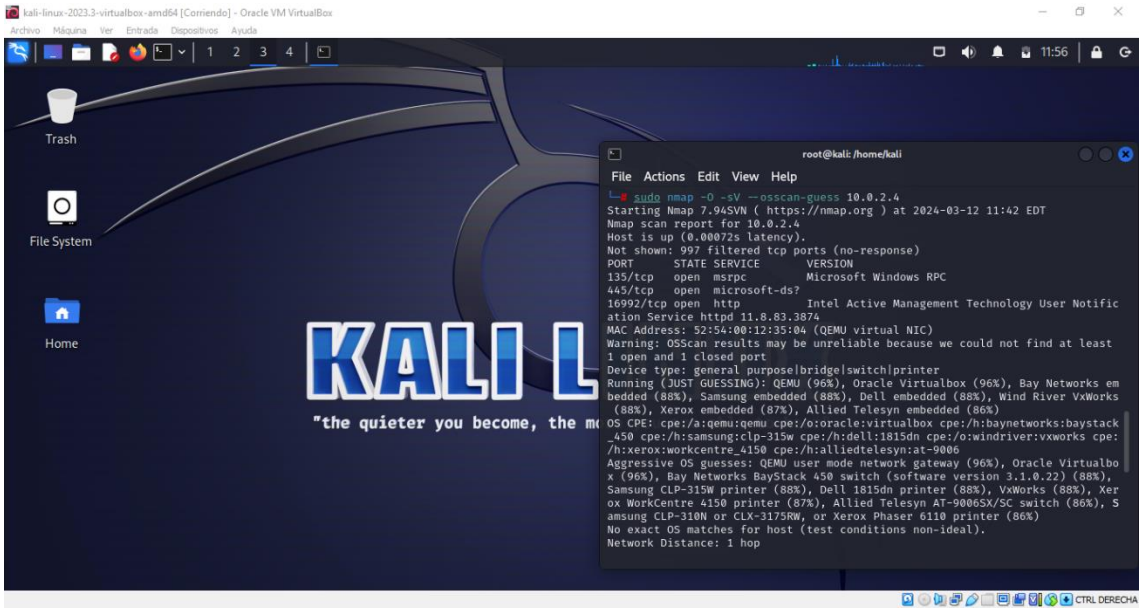
Se evidencia el escaneo de vulnerabilidades.

Figura 20 Escaneo



Fuente: Elaboración propia.

Figura 21 Configuración

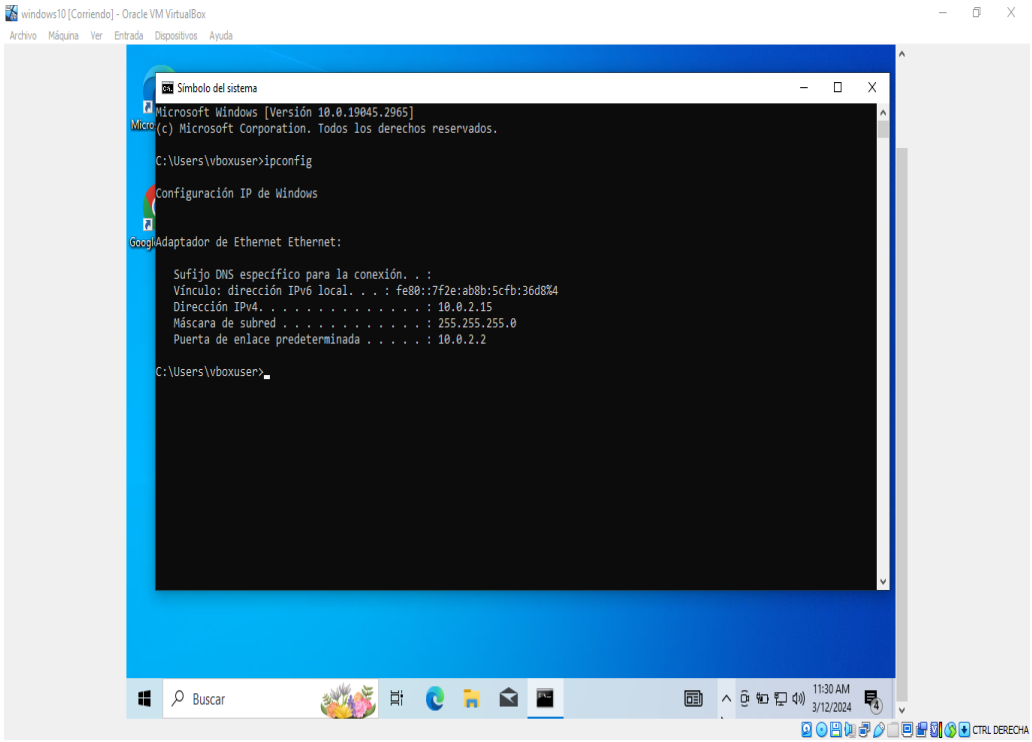


Fuente: Elaboración propia.

Figura 22 ejecución

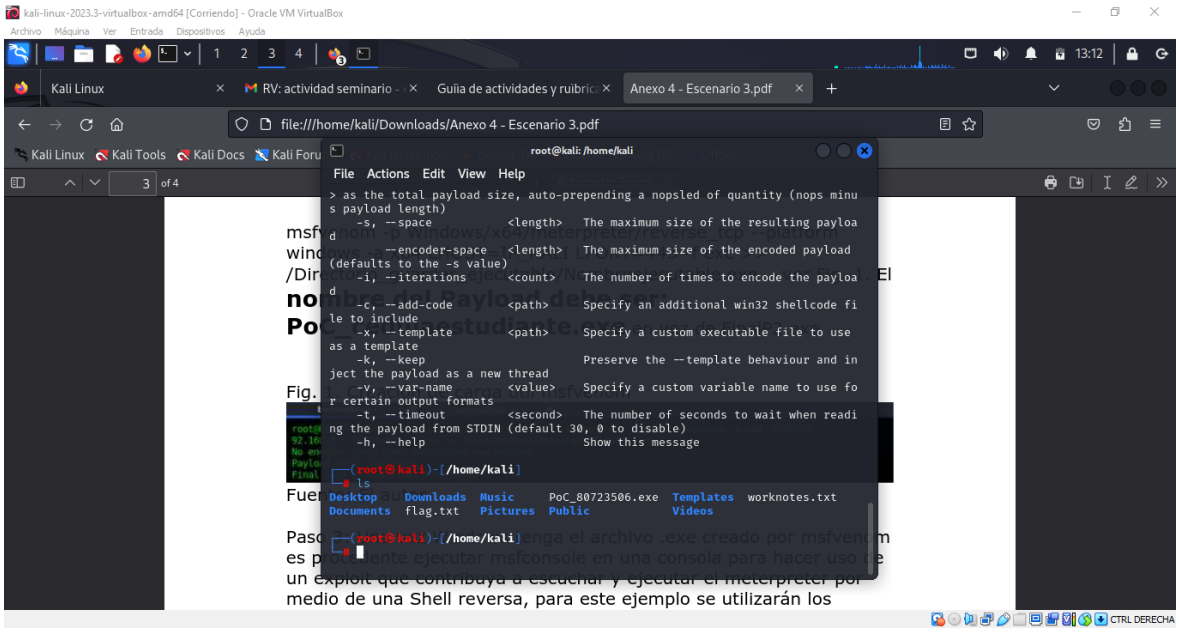
Fuente: Elaboración propia.

Figura 23 Acceso



Fuente: Elaboración propia.

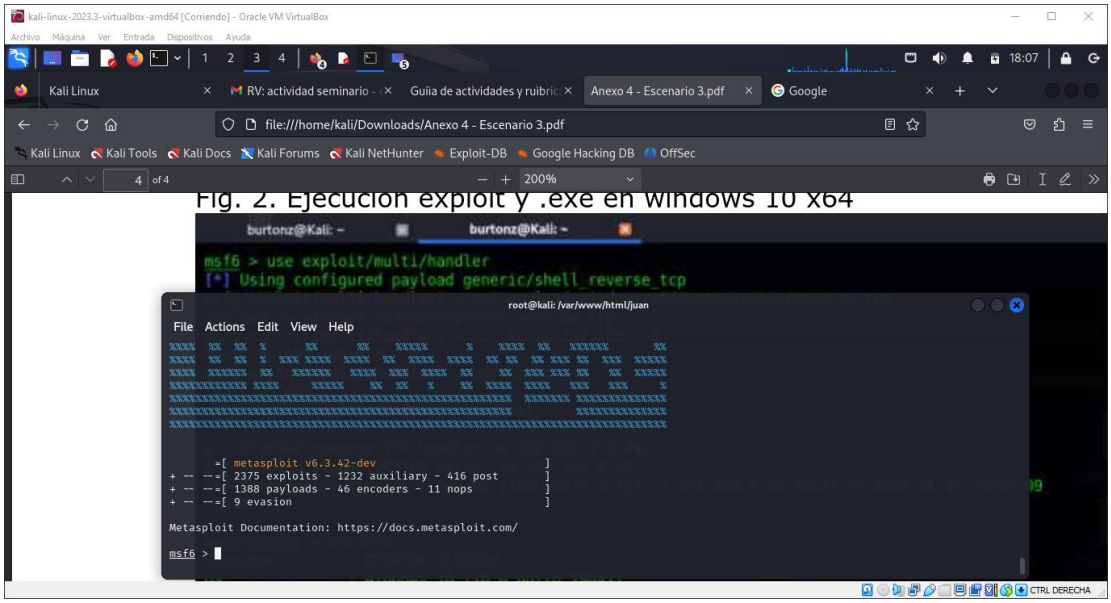
Figura 24 Acceso 2



Fuente: Elaboración propia.

Evidenciamos la ejecución de la herramienta metaexploit.

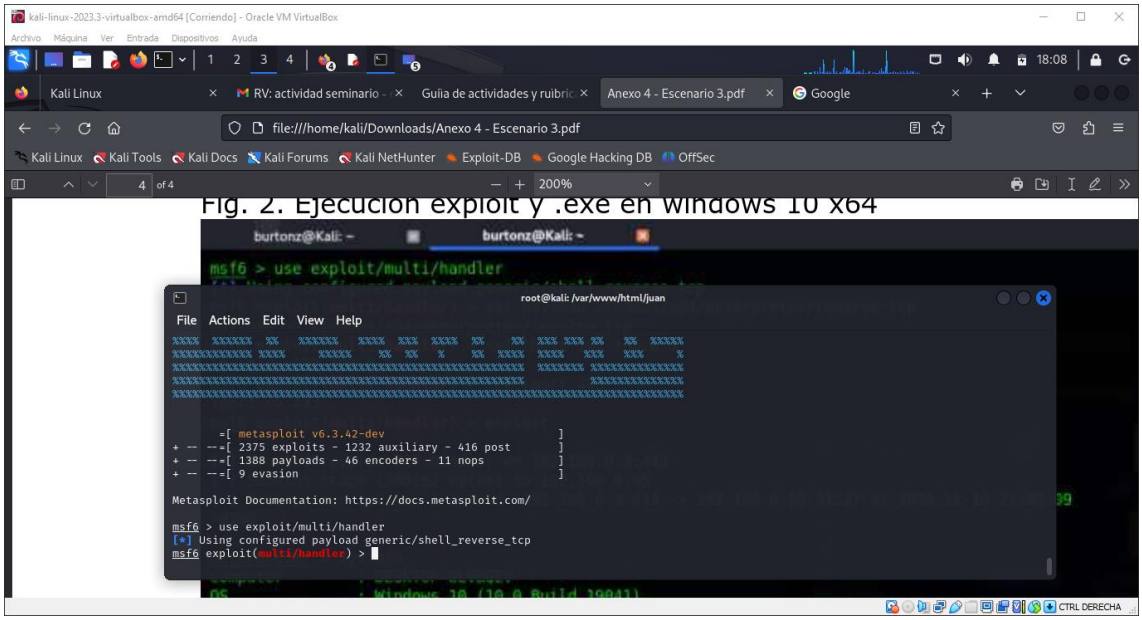
Figura 25 Ejecución herramienta



Fuente: Elaboración propia.

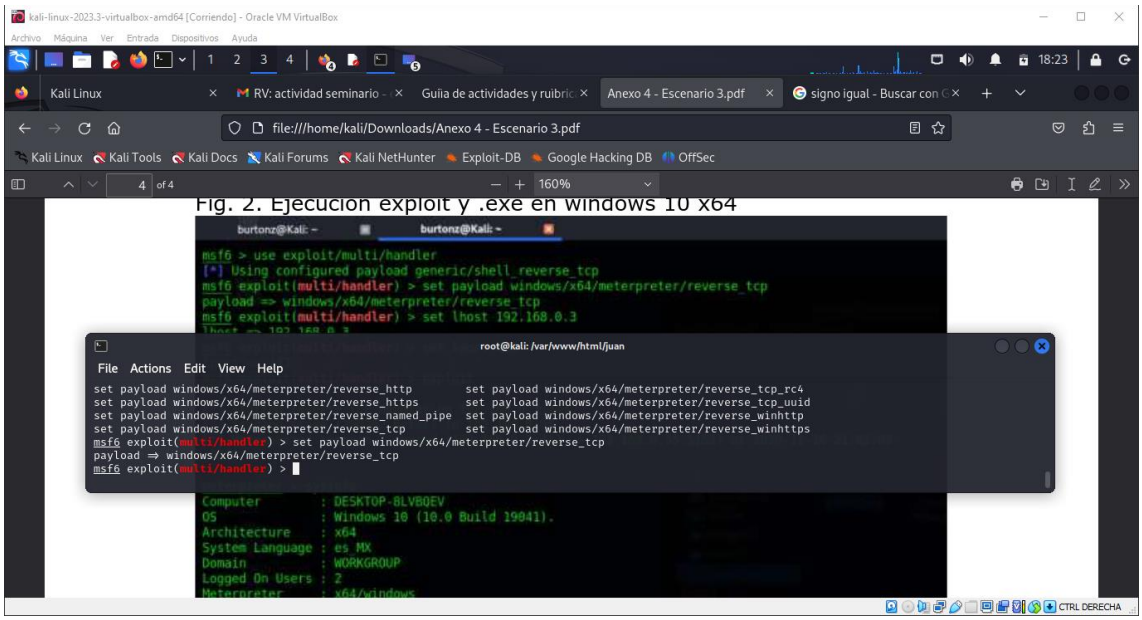
Se ejecuta el comando propuesto para obtener el acceso a la máquina Windows.

Figura 26 Comandos herramienta



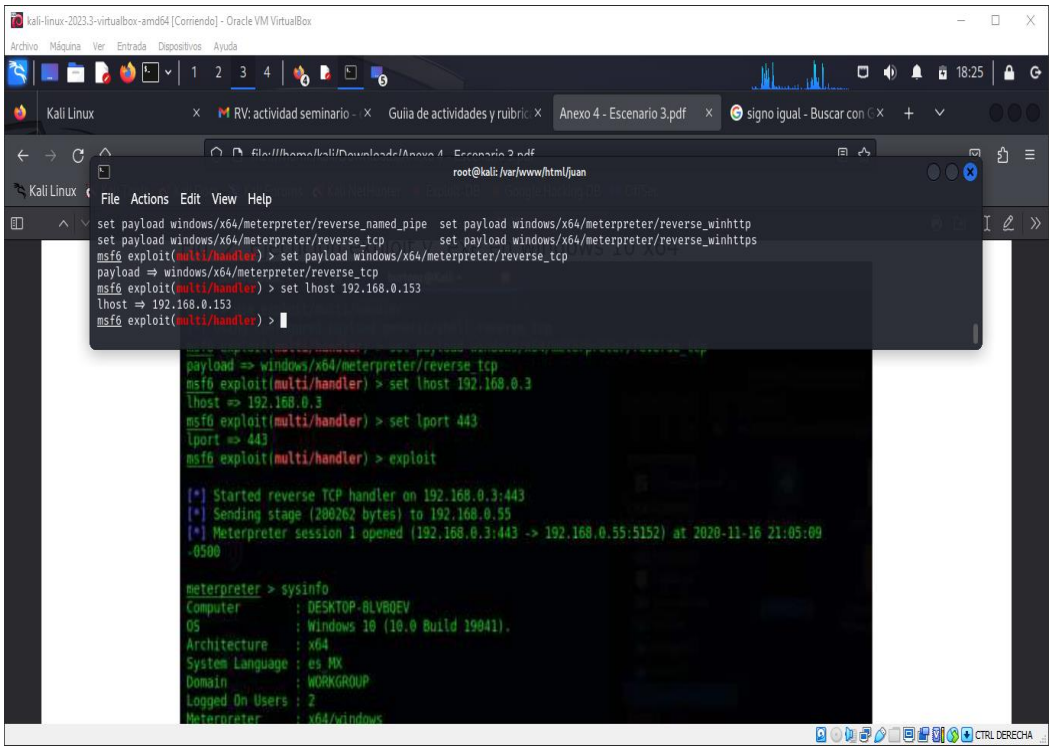
Fuente: Elaboración propia.

Figura 27 Comandos herramienta 2



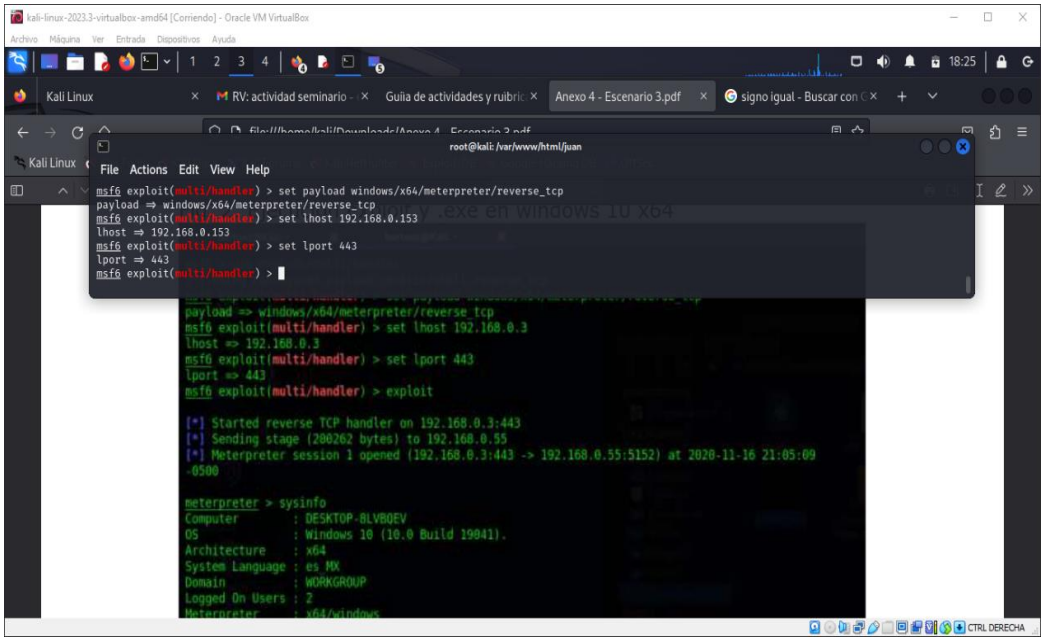
Fuente: Elaboración propia.

Figura 28 Ingreso



Fuente: Elaboración propia.

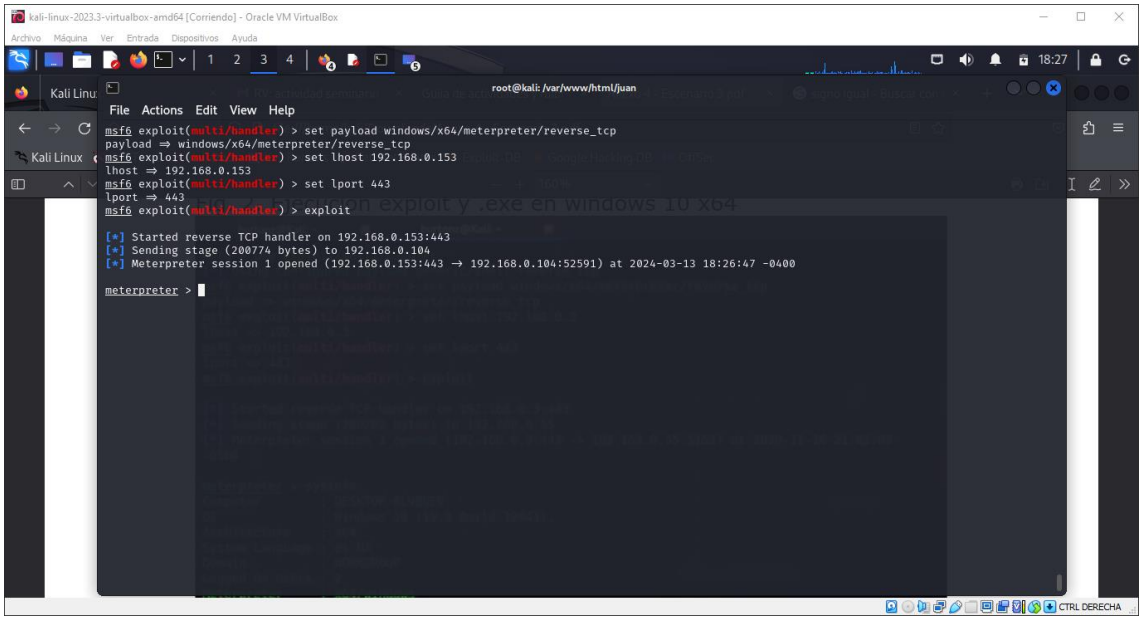
Figura 29 Control



Fuente: Elaboración propia.

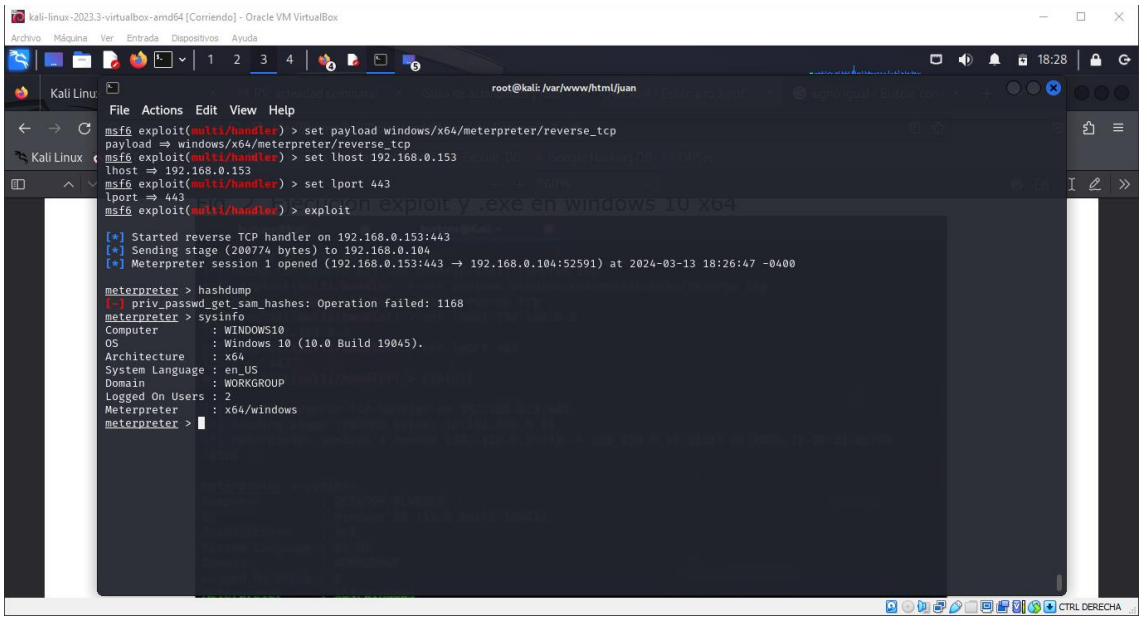
Obtenemos el acceso remoto a la maquina Windows.

Figura 30 Control de la maquina Windows



Fuente: Elaboración propia.

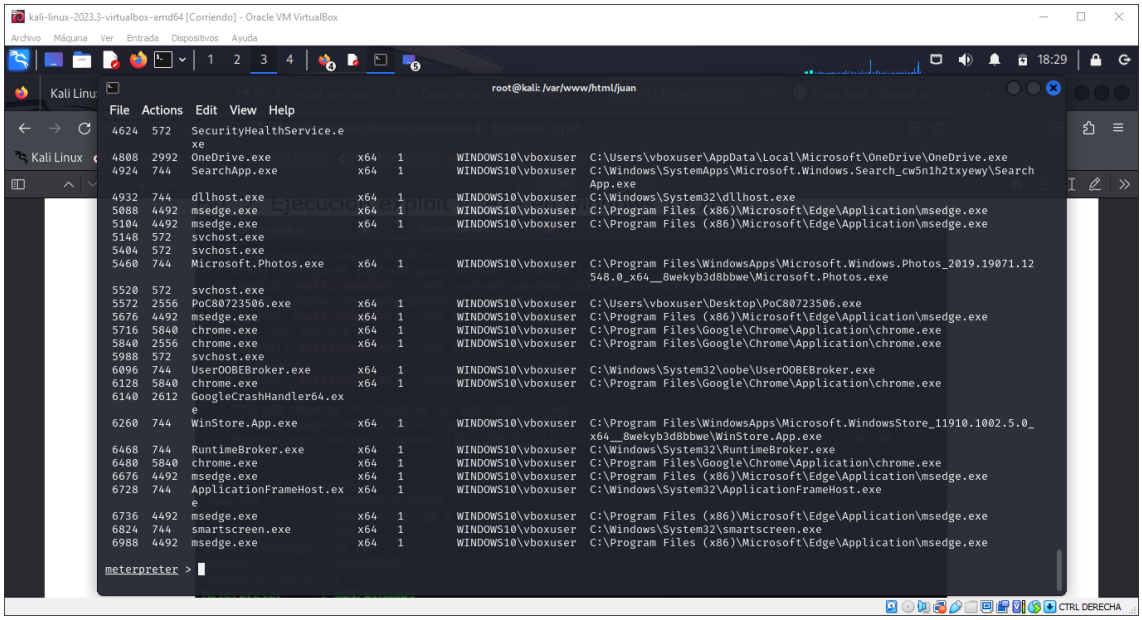
Figura 31 Control de la maquina



Fuente: Elaboración propia.

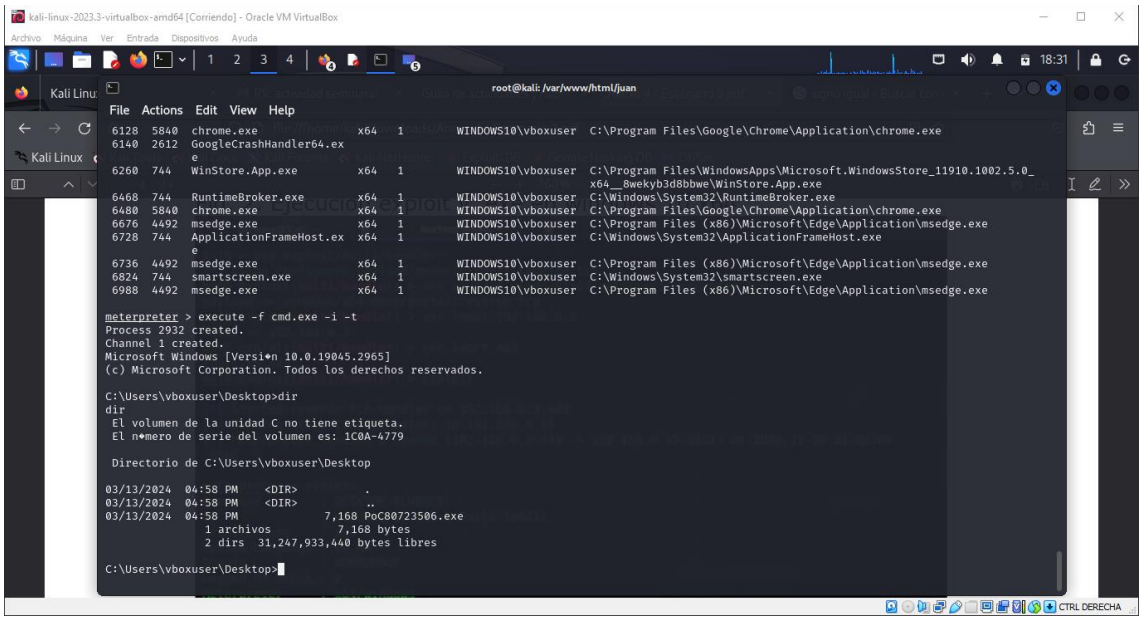
Ejecutamos comandos con privilegios de administrador.

Figura 32 Privilegios



Fuente: Elaboración propia.

Figura 33 Ejecución



Fuente: Elaboración propia.

6 ESCENARIO 4

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

Evaluar el incidente. Es necesario identificar y evaluar la gravedad del impacto del incidente, llevando un registro detallado de los sistemas y procesos afectados y la continuidad o no del impacto.

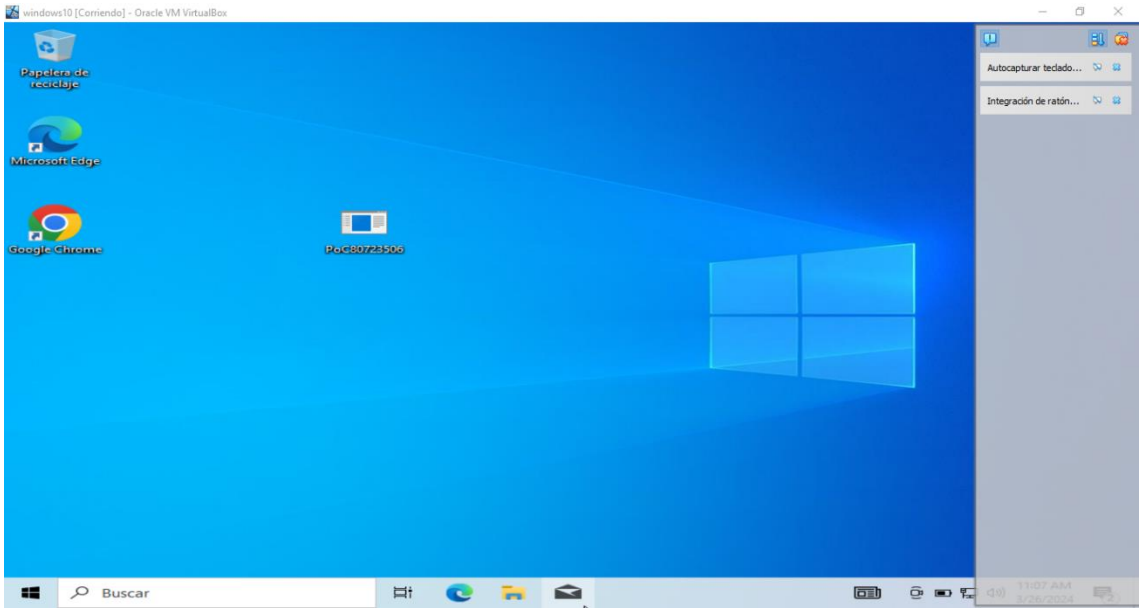
Informar del incidente. Es necesario tener compartimentación de la información con prudencia, de manera que solo se entere las personas autorizadas, toda vez que puede existir un insider, involucrado, y puede afectar la gestión del incidente.

Contener los daños. Es de extrema importancia realizar de manera oportuna la gestión del incidente, que permita ser efectivo de manera diferencial, priorizando las acciones según la manera de ponderar los recursos afectados entre persona, información y equipos tecnológicos afectados.

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

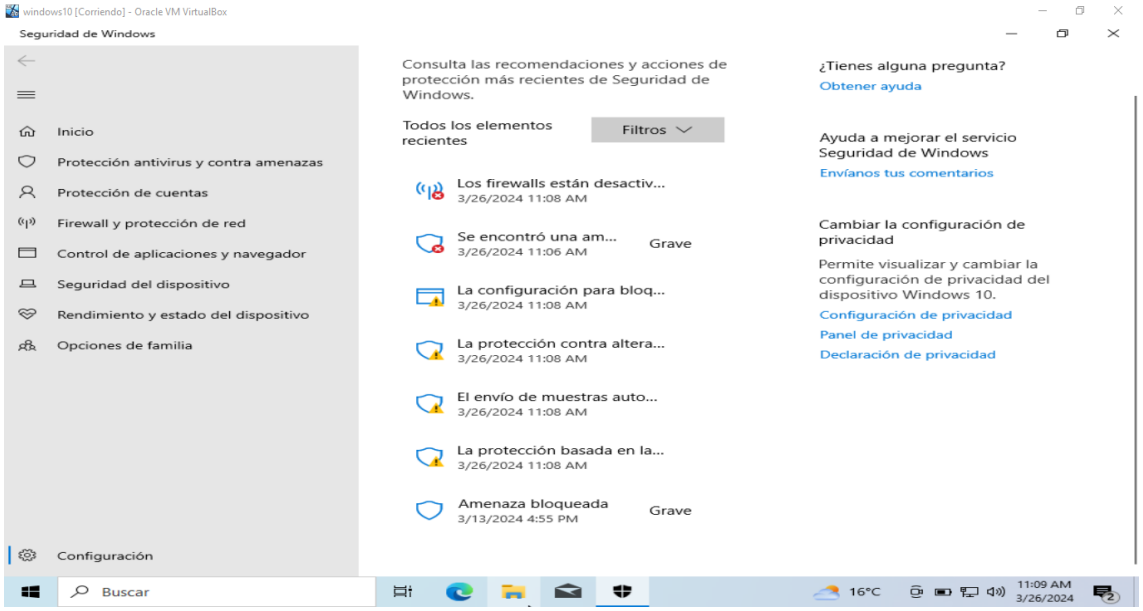
Con el propósito de hardenizar las máquinas virtual con Windows, tenemos necesariamente que verificar y activar todas las herramientas de seguridad que posee el sistema operativo, Windows defender y los firewall, los cuales están pre instalados con los requisito necesarios para el propósito, en el cual se deben configurar las actualizaciones y los respectivos parches de seguridad que tiene destinados él y otorgados por Microsoft, se realiza la revisión de puertos los cuales necesariamente toca tener habilitados si el fin del equipo es mantener conexión con otros equipos y redes, se ejecutan las actualizaciones vigentes en ese entendido los atacantes no lograran utilizar ese puerto, se verifica nuevamente los sistemas de seguridad y la activación de los mismos, focalizadas en desactivar las opciones que permitían las conexiones con asistencia remota, toda vez que esta conexión fue la que permitió el ataque, de manera que a partir de ahora se instalen los parches, al realizar esta configuración se encuentran las actualizaciones requeridas las cuales son instaladas y que no tienen costo, si se quisiera una harderizacion más fuerte se podría contratar servicios de pago para obtener mayor eficiencia y eficacia.

Figura 34 Payload



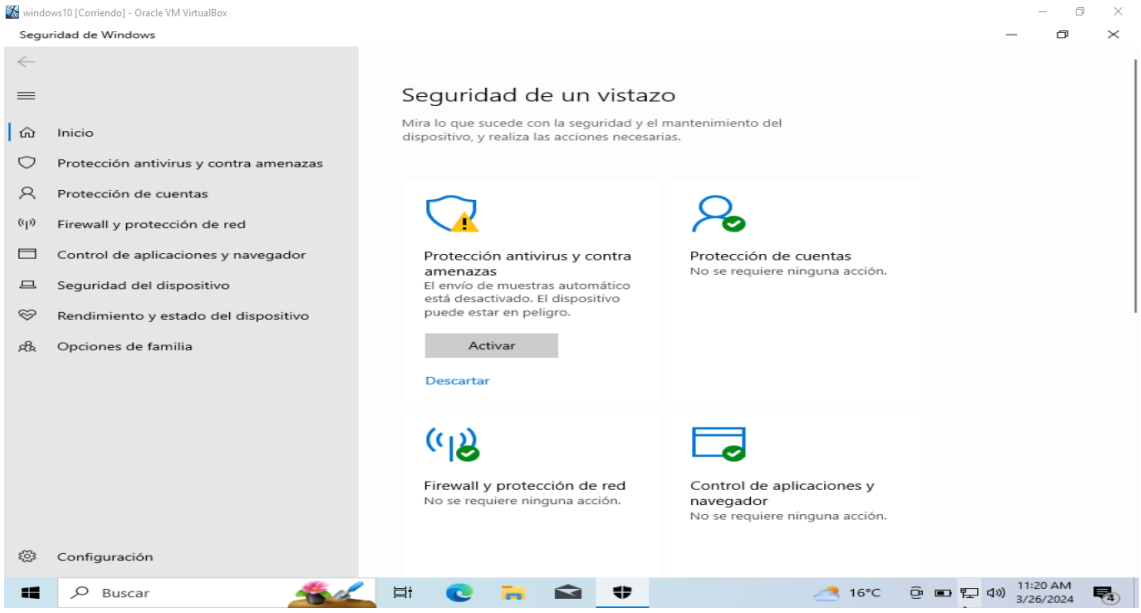
Fuente: Elaboración propia.

Figura 35 Configuración de seguridad



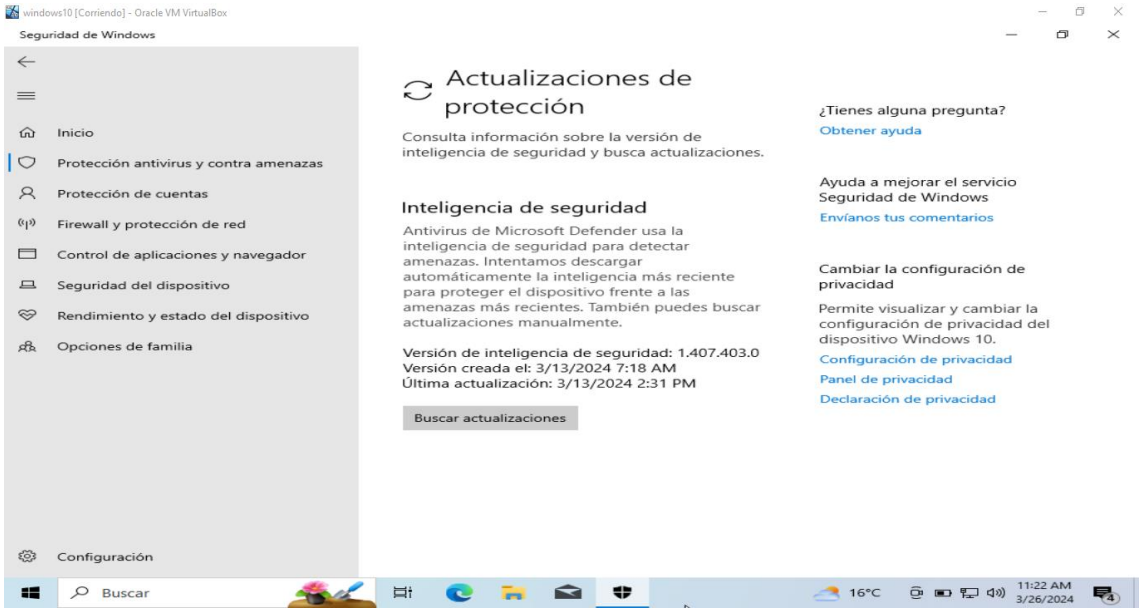
Fuente: Elaboración propia.

Figura 36 Activación



Fuente: Elaboración propia.

Figura 37 Resultado



Fuente: Elaboración propia.

6.3. ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS ANTES MENCIONADOS CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Los equipos de blue y red team, tienen propósitos comunes pero existen momentos donde no se evidencia una sinergia entre los dos equipos, lo que conlleva a que no se comparta la información requerida que genera una competencia que puede afectar la entidad o empresa, toda vez que no comparten la información necesaria, es de esta manera que el equipo purple team, es el equipo de reunir y sincronizar tener las suficiente retroalimentación entre los dos equipos de manera que se optimice la información de cada uno de los equipos de ataque y de defensa.

Este equipo lidera que los equipos de red y blue team, trabajen de manera coordinada, a través del intercambio constante de recursos, metodologías procesos y herramientas.[5]

6.4. ¿QUÉ FUNCIÓN TIENE CIS "CENTER FOR INTERNET SECURITY" DENTRO DE EQUIPOS BLUETEAM?

Obedece a los Controles de Seguridad Críticas y se relaciona con las buenas prácticas efectivas, aprobadas y certificadas, que contribuyen al mejoramiento en niveles de ciberseguridad a las organizaciones y entidades, en la que se incluyen las recomendaciones más importantes de defensa de los sistemas informáticos, las cuales se dividen en tres pilares principales: las básicas, las fundamentales y las organizacionales.

Estas estrategias practicas son reconocidas a nivel mundial para proteger lis sistemas informáticas y principalmente los datos como el activo más valioso de las organizaciones, otorgando entornos seguros tanto de manera local como con aplicaciones en la nube.

NIVELES DE SEGURIDAD CIS

En cuanto a los niveles tenemos:

[5]RED TEAM, Blue Team y Purple team: Guía completa sobre los equipos en Ciberseguridad [Ordoñez, W.]. Ciberseguridad, tecnología e innovación | GroupHacking [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/

Nivel 1: configuración de seguridad mínima recomendada. Debería configurarse en cualquier sistema, sin importar su tamaño. Causa poco o ningún impacto en el servicio o en una funcionalidad reducida.
Nivel 2: configuración de seguridad recomendada para entornos de alta seguridad. Podría dar lugar a una cierta reducción de la funcionalidad.

Controles CIS para gestionar tecnologías

En lo que respecta a las categorías nos podemos encontrar con benchmarks de:

- Sistemas operativos. Que cubren las configuraciones de seguridad de los principales sistemas: Windows, Linux, OSX…

- Software de servidores. Sirven para implementar configuraciones de seguridad en los softwares de servidores más usados: Microsoft SQL Server, Nginx, MySQL…

- Proveedores cloud. Se centran en las configuraciones de seguridad de las nubes más importantes: Amazon Web Services, Microsoft Azure, Google Cloud…

- Dispositivos móviles. Focalizados en los sistemas operativos móviles, incluyendo, por supuesto, Android e iOS.

- Dispositivos red. Recogen un conjunto de recomendaciones generales y específicas para los dispositivos red y hardware aplicables como Cisco, F5 o Palo Alto Networks.

- Software de escritorio. Se ocupan de la configuración de seguridad de los programas de escritorio más usados como Microsoft Office, Google Chrome o Safari Browser.

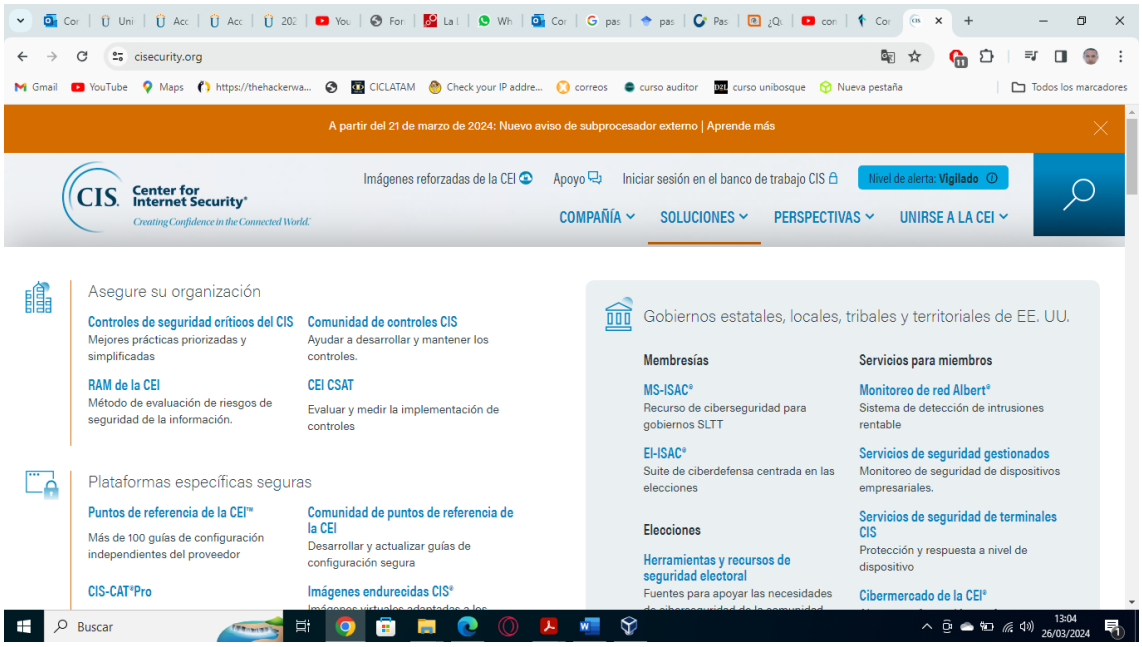
- Dispositivos de impresión multifunción. Incluyen recomendaciones para configurar impresoras multifunción en entornos de oficinas.
- Al categorizar los benchmarks, se facilita el acceso a los mismos, sistematizándolos de forma altamente intuitiva.

El equipo de Tarlogic Security emplea las guías CIS de forma habitual para verificar los dos niveles de configuración de la seguridad en tecnologías concretas como Windows 10, Microsoft 365, servidores Linux, bases de datos

Figura 38 pagina consulta

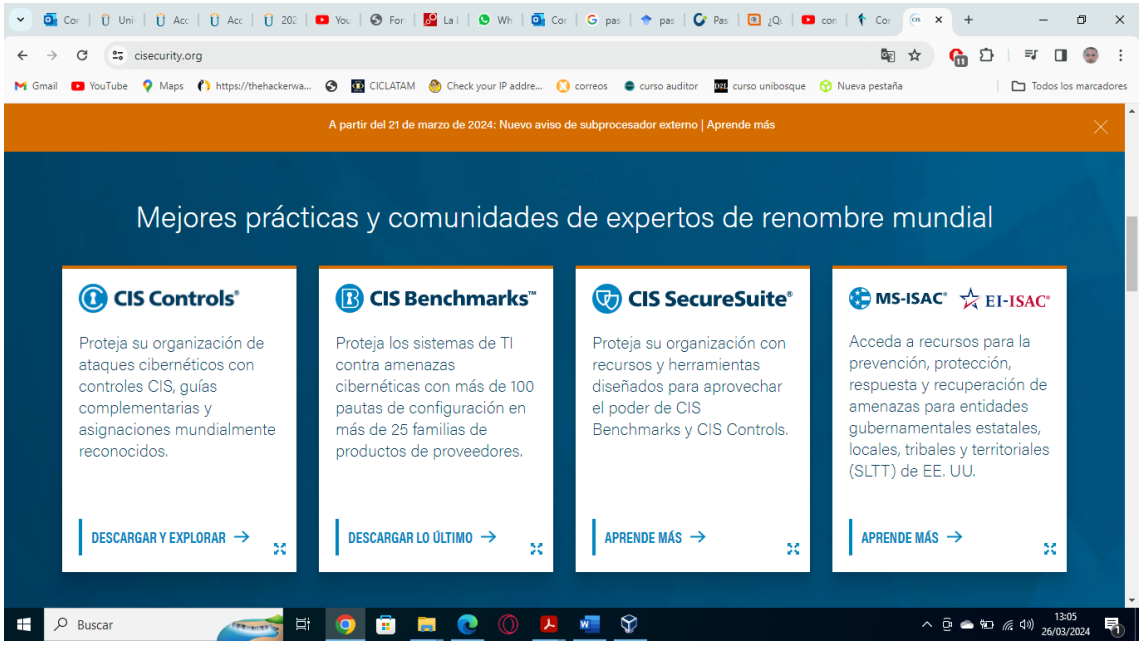
Fuente: Elaboración propia.

Figura 39 Complemento



Fuente: Elaboración propia.

Figura 40 Recursos



Fuente: Elaboración propia.

6.5. TABLA DE DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR.

Tabla 1 Diferencias existentes entre: SIEM y XDR.

N°	SIEM	XDR
1	Permiten a las organizaciones actuar de manera inmediata y eficiente ante los ciberataques con el objetivo de afectar los sistemas de información que estas poseen.	Tecnología de seguridad multicapa que protege la infraestructura de TI
2	Recopila la mayor cantidad de información de los dispositivos y aplicaciones en una base de datos para analizarla y así poder detectar comportamientos anómalos y no habituales en la red que permiten detectar vulnerabilidades o amenazas y bloquearlas	Recopila y correlaciona los datos de múltiples capas de seguridad, incluidos los end points, las aplicaciones, el correo electrónico, las nubes y las redes, para proporcionar una mayor visibilidad del entorno tecnológico de una organización

N°	SIEM	XDR
3	Combina dos tecnologías de seguridad anteriores las cuales son administración de eventos de seguridad (SEM) la cual detecta patrones de acceso fuera de lo común en tiempo real, y la otra es la administración información de seguridad (SIM), esta centraliza los registros de seguridad para una interpretación inmediata	Su enfoque va más allá de la infraestructura de TI, ya que incorpora datos de otras fuentes, como es los correo electrónico y servicios en la nube.
4	Se centra en la recopilación, correlación y análisis de registros y eventos de seguridad de múltiples fuentes en toda la infraestructura de TI de una organización.	identificar las amenazas, responder a ellas y resolverlas más rápidamente, incluso todo esto puede generar una reducción en los costos de una filtración de datos de las organizaciones que deciden implementar

Fuente: Elaboración propia.

6.6. 3 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL.

Snort: es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real.

Snort está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.[6]

Este IDS implementa un lenguaje de creación de reglas flexibles, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, DDoS, finger, ftp, ataques web, CGI, escaneos Nmap,

[6] SNORT. network intrusion detection & prevention system. [Anónimo]. Snort.org [página web]. [Consultado el 19, febrero, 2024]. Disponible en Internet: https://www.snort.org

Puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS).

Nmap: es la mejor herramienta de escaneo de puertos y descubrimiento de hosts que existe actualmente. Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red, es capaz de escanear qué hosts están levantados, e incluso comprobar si tienen algún puerto abierto, si están filtrando los puertos (tienen un firewall activado), e incluso saber qué sistema operativo está utilizando un determinado objetivo.

Al navegar por la red, al utilizar equipos conectados, podemos sufrir muchos tipos de ataques que de una u otra forma nos pueden comprometer. Estamos expuestos constantemente y por ello es importante conocer los riesgos que pueden afectarnos. Este tipo de ataque también se conoce como port scan. Básicamente lo que hace un atacante es analizar de forma automática todos los puertos de un equipo, como por ejemplo un ordenador, que esté conectado a la red. Lo que buscan es detectar posibles puertos abiertos y cuáles podrían tener protocolos de seguridad deficientes.

Herramienta AIDE (Advanced Intrusion Detection Environment). Es la herramienta que nos a escanear sistemas de archivos con el propósito de buscar cambios no autorizados y va generando alertas si detecta modificaciones sospechosas. Es importante si se procura la detección de intrusiones basada en el sistema de archivos.

La manera en que puede realizar esa detección de cambios es que AIDE crea una base de datos de archivos en la ejecución inicial y luego se comprueba con dicha base de datos en las siguientes ejecuciones.

Debemos tener en cuenta en esta herramienta es que la base de datos que crea inicialmente se almacena en el sistema de archivos raíz, y un atacante podría modificarla fácilmente para buscar ocultar su intrusión al sistema, es por esto por lo que se recomienda realizar una copia de la base de datos y realizar comprobaciones contra dicha copia periódicamente.

7 APORTES DENTRO DE UNA ORGANIZACIÓN

Fortalecer los procesos que contribuya a la reducción de los riesgos, se establecieron instrumentos de recolección de información los cuales, permiten establecer los parámetros esenciales para estructurar de una manera adecuada y acorde a las necesidades, recopilando información de expertos en ciberseguridad, para continuar analizando los datos recopilados se tomó la frecuencia de las estrategias implementadas por equipos de Blue Team después de realizar cuantificación y la decodificación de los instrumentos de recolección de información.

El análisis consistió en definir cada una de las buenas y malas prácticas en el parcheo de aplicaciones, focalizándose en sus componentes tecnológicos que permitan las conexiones de los equipos terminales con los servidores y a su vez la trasmisión en tiempo real de la información, Partiendo que para poder materializar este tipo de proyectos se requiere del despliegue de equipos capacitados y protocolos, planeación y secuencia de actividades periódicas en concordancia con la periodicidad de los análisis d ellos programas de acuerdo a su impacto y riesgo analizado.

8 RECOMENDACIONES Y POLITICAS DE MEJORA EN ENTORNOS T.I.

Para fortalecer los procesos que contribuya a la reducción de los riesgos, se establecieron instrumentos de recolección de información los cuales, permiten establecer los parámetros esenciales para estructurar de una manera adecuada y acorde a las necesidades, recopilando información de expertos en ciberseguridad, para continuar analizando los datos recopilados se tomó la frecuencia de las estrategias implementadas por equipos de Blue Team después de realizar cuantificación y la decodificación de los instrumentos de recolección de información.

9 CONCLUSIONES SOBRE LA INVERSIÓN EN CIBERSEGURIDAD EN LAS ORGANIZACIONES

Con el equipo un Blue Tea focalizado en gestionar las debilidades del sistema, a la entidad siempre estará acompañada de soluciones oportunas que garanticen menor porcentaje de riesgo dedicado a tratar las fragilidades del sistema de su empresa, sus soluciones de ciberseguridad tienden a acompañar siempre las innovaciones del mercado, o que garantizan menor vulnerabilidad de su negocio a los ataques.

La gestión de los equipos debe ser realizada periódicamente analizando la eficiencia de las practicas medidas o políticas que se adoptan en una organización, con el propósito de mitigar la recurrente exposición al riesgo, de manera que se esté revisando, identificando y actualizando todos los softwares de uso de la entidad.

10 CONCLUCIONES

La gestión de los equipos debe ser realizada periódicamente analizando la eficiencia de las practicas medidas o políticas que se adoptan en una organización, con el propósito de mitigar la recurrente exposición al riesgo, de manera que se esté revisando, identificando y actualizando todos los softwares de uso de la entidad.

1-Inventario de Dispositivos Autorizados y No Autorizados

Todos los dispositivos de hardware en la red para que solo los autorizados se les da acceso a los dispositivos, y se encuentran dispositivos no autorizados y no administrados y se les impide obtener acceso.

2 - Inventario de Software Autorizado y No Autorizado

Administrar activamente (inventario, seguimiento y corrección) todo el software en la red para que solo el software autorizado sea instalado y pueda ejecutarse, y que se encuentre software no autorizado y no administrado y se impida su acceso instalación o ejecución.

3 - Configuraciones seguras para hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y Servidores.

Establecer, implementar y gestionar activamente (seguir, informar, corregir) la configuración de seguridad de las computadoras portátiles, servidores y estaciones de trabajo mediante un riguroso proceso de gestión de configuración y control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

4 - Evaluación y corrección continua de vulnerabilidades

Adquirir, evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar, y minimizar la ventana de oportunidad para los atacantes.

5 - Defensas contra malware

Controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la empresa, mientras optimizar el uso de la automatización para permitir

una rápida actualización de la defensa, recopilación de datos y acciones correctivas.

51

6 - Seguridad del software de aplicaciones

Gestionar el ciclo de vida de seguridad de todo el software desarrollado y adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad.

7 - Control de acceso inalámbrico

Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso de seguridad de las redes de área local inalámbricas, (LANS), puntos de acceso y sistemas de clientes inalámbricos.

8 - Capacidad de recuperación de datos

Los procesos y herramientas utilizados para realizar copias de seguridad adecuadas de la información crítica con una metodología comprobada para realizar copias de seguridad oportunas recuperación del mismo.

9 - Evaluación de habilidades de seguridad y capacitación adecuada para llenar vacíos para todos los roles funcionales de la organización (priorizando aquellos de misión crítica para el negocio y su seguridad), identificar los conocimientos, habilidades y capacidades específicos necesarios para apoyar la defensa de la empresa; desarrollar y ejecutar un plan integrado para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, programas de formación y sensibilización.

10 - Configuraciones seguras para dispositivos de red como firewalls, enrutadores y conmutadores, establecer, implementar y gestionar activamente (seguir, informar, corregir) la configuración de seguridad de la red dispositivos de infraestructura utilizando un riguroso proceso de gestión de configuración y control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

11 - Limitación y Control de Puertos, Protocolos y Servicios de Red

Gestionar (rastrear/controlar/corregir) el uso operativo continuo de puertos, protocolos y servicios en red de dispositivos para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

12 - Uso Controlado de Privilegios Administrativos

Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso, asignación y configuración de privilegios administrativos en computadoras, redes y aplicaciones.

11 RECOMENDACIONES

Las deficiencias dejaron a las aplicaciones expuestas a ataques y vulnerabilidades durante períodos prolongados, lo que puso en peligro la confidencialidad, integridad y disponibilidad del dato y sistema.

• Las evaluaciones para las fallas y deficiencias en las prácticas de parcheo de aplicaciones revelaron varios desafíos que deben abordarse para optimizar la seguridad y protección del sistema y el dato.

• Los retrasos de la aplicación de parches, la falta de priorización adecuada, la falta de pruebas exhaustivas, la incapacidad para identificar y priorizar vulnerabilidades, sumada a la falta de automatización, son áreas críticas que requieren atención.

• Al abordar estas deficiencias, el equipo de Blue Team se logró encontrar estrategias que puedan fortalecer su capacidad de respuesta, reducir los riesgos y asegurar una protección más efectiva de los sistemas.

• Se analizó la imperiosa necesidad de fortalecer el componente tecnológico en de los equipos de Blue Team, incluyendo servicios de almacenamiento en nube, infraestructura de fibra óptica y banda ancha, entre otras que permitan asegurar los procesos y procedimientos que se adelantan y a su vez blinden actualizaciones e intercambio de data que realicen las entidades.

BIBLIOGRAFIA

ALLEN M. Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM. Biblioteca virtual UNAD [página web]. [Consultado el 18, febrero, 2024]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

ALVAREZ V. Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar [página web]. [Consultado el 19, febrero, 2024]. Disponible en Internet: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

ARROYO GUARDEÑO D. GAYOSO MARTÍNEZ V. & HERNÁNDEZ ENCINAS L. Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. Biblioteca virtual UNAD [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

ARROYO GUARDEÑO D., GAYOSO MARTÍNEZ V., & HERNÁNDEZ ENCINAS L. Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. Biblioteca virtual UNAD [página web]. [Consultado el 23, marzo, 2024]. Disponible en Internet: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. [Consultado el 27, abril, 2024]. Disponible en Internet: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CONVENIO SOBRE La Ciberdelincuencia [Anónimo]. OAS - Organization of American States: Democracy for peace, security, and development [página web]. [Consultado el 20, marzo, 2024]. Disponible en Internet: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

ESTRATEGIAS FUNDAMENTALES de seguridad informática [Anónimo]. ARATECNIA SISTEMAS Y SERVICIOS [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://aratecnia.es/seguridad-informatica-estrategias-fundamentales/

ELABORACIÓN DE la política general de seguridad y privacidad de la información [Anónimo]. Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic. [página web]. [Consultado el 7, marzo, 2024]. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

ELABORACIÓN DE la política general de seguridad y privacidad de la información, 17-24. [Anónimo]. Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic. [página web]. [Consultado el 27, marzo, 2024]. Disponible en Internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

¿QUÉ ES Blue Team en Ciberseguridad? | KC [Anónimo]. KeepCoding Bootcamps [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

¿QUÉ ES una vulnerabilidad en seguridad informática? Ejemplos [Anónimo]. Blog HostDime Perú, Servidores dedicados [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/

GLOSARIO de Ciberseguridad | MNEMO [Anónimo]. MNEMO | Ciberseguridad, Transformación Digital [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://mnemo.com/glosario-ciberseguridad/

ISO 27002 Tecnología de la información - técnicas de seguridad [Anónimo]. Accelerating progress towards a sustainable world | BSI [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://www.bsigroup.com/es-ES/iso-27002-controles-de-seguridad-de-la-informacion/

LEY 1273 [Anónimo]. Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic [página web]. [Consultado el 27, marzo, 2024]. Disponible en Internet: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

LEY 1581 [Anónimo]. Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic. [página web]. [Consultado el 15, marzo, 2024]. Disponible en Internet: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

LEY_1273_2009 [Anónimo]. Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic [página web]. [Consultado el 27, marzo, 2024]. Disponible en Internet: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

LEY_1581_2012 [Anónimo]. Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic [página web]. [Consultado el 28, marzo, 2024]. Disponible en Internet: https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

PRINCIPIOS BÁSICOS de la seguridad de la información - OSTEC | Segurança digital de resultados [Anónimo]. OSTEC | Segurança digital de resultados [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://ostec.blog/es/seguridad-informacion/principios-basicos-de-la-seguridad-de-la-informacion/

¿QUÉ ES Blue Team en Ciberseguridad? | KC [Anónimo]. KeepCoding Bootcamps [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

RED TEAM, Blue Team y Purple team: Guía completa sobre los equipos en Ciberseguridad [Anónimo]. Ciberseguridad, tecnología e innovación | GroupHacking [página web]. [Consultado el 15, febrero, 2024]. Disponible en Internet: https://www.grouphacking.com/ciberseguridad/hacking-etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-en-ciberseguridad/

SNORT. network intrusion detection & prevention system. [Anónimo]. Snort.org [página web]. [Consultado el 19, febrero, 2024]. Disponible en Internet: https://www.snort.org

SENADO de la República de Colombia. (s/f). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. [Sitio web]. [Consultado: 15 de febrero de 2024]. Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

VILMA, Alvarez. Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar [página web]. [Consultado el 27, marzo, 2024]. Disponible en Internet: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

ANEXOS

LINK DEL VIDEO

https://www.youtube.com/watch?v=93pqaaln3uI&ab_channel=CercadoBeltr%C3%A1nPaula

RESULTADOS DE LA PRUEBA ANTI-PLAGIO