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

JENNY ZORAIDA HERRERA MELO

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

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

JENNY ZORAIDA HERRERA MELO

Nombre
Luis Fernando Zambrano

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

CONTENIDO

pág.

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

AMENAZA: Son las acciones que puede realizar un tercero para aprovechar las vulnerabilidades del sistema y cometer un ataque, que puede llegar a la denegación de servicio o afectaciones en el mismo.

BLUE TEAM: Equipo encargado de analizar la seguridad de una organización, con la finalidad de realizar Hardening a los sistemas y responder ante un posible ataque de seguridad.

EXPLOIT: Es un software que aprovecha cualquier brecha de seguridad, previa la realización de por ejemplo la ingeniería social.

FOOTPRINTING: Es una técnica que se utiliza para recolectar información pública, que no es necesario la interacción con el objetivo.

HARDENING: Aseguramiento del sistema para evitar o minimizar los ataques.

MSFVENOM: Herramienta para la creación de Payload, generando cargas útiles para varios sistemas operativos.

RED TEAM: Equipo encargado de realizar ataque a los sistemas de información de una organización, haciendo uso de herramientas para la búsqueda de Vulnerabilidades.

PAYLOAD: Es parte de un Malware cuyo objetivo es realizar una acción maliciosa.

VULNERABILIDAD: Debilidad encontrada en los sistemas de información, esta se puede presentar a nivel de Software o hardware, comprometiendo la seguridad de las organizaciones.

RESUMEN

Por medio del siguiente informe técnico, se pretende dar a conocer las capacidades técnicas, legales y la gestión de los equipos red team y blue team, en las organizaciones, con la finalidad de entender los aspectos más relevantes y el funcionamiento de estos, para minimizar los impactos y construir un plan de mejoramiento continuo, en cuanto a la seguridad de los sistemas informáticos.

En primera instancia se da a conocer las leyes que salvaguardan la información, como los son la ley 1273 de 2009, que protege y preserva los sistemas que manejan tecnologías de la información, donde se tipifican como delitos una serie de hechos con el manejo de los datos y la ley 1581 de 2012 en donde se regula el tratamiento y recolección de los datos personales.

Como segunda instancia, logramos realizar un laboratorio en un ambiente controlado donde se realizaba la indagación sobre un caso de ingreso no autorizado al sistema y manipulación de un archivo relevante para el usuario, utilizando las herramientas Msfvenom, Payload y exploit entre otros, realizado por el grupo Red Team y para contrarrestar el ataque se trabajó como equipo Blue Team con la finalidad de realizar Hardening en el equipo afectado.

Como tercera instancia, se generaron recomendaciones, para la aplicación de los grupos Read Team y Blue Team y aprovechar todo el conocimiento y seguridad que estos pueden implementar en las organizaciones, ya que en la actualidad es muy importante la ciberseguridad.

Palabras claves: Amenaza, Exploit, Hardening, Msfvenom, Payload

ABSTRACT

Through the following technical report, it is intended to make known the technical, legal and management capabilities of the red team and blue team in organizations, in order to understand the most relevant aspects and their operation, to minimize the impacts and build a continuous improvement plan, regarding the security of computer systems.

In the first instance, the laws that safeguard information are announced, such as law 1273 of 2009, which protects and preserves the systems that manage information technologies, where a series of events with the management of information are classified as crimes. Data and law 1581 of 2012 which regulates the processing and collection of personal data.

As a second instance, we managed to carry out a laboratory in a controlled environment where the investigation was carried out on a case of unauthorized entry to the system and manipulation of a file relevant to the user, using the tools msfvenom, payload and exploit among others, carried out by the red team group and to counter the attack we worked as a blue team with the purpose of performing hardening on the affected team.

As a third instance, recommendations were generated for the application of the read team and blue team groups and take advantage of all the knowledge and security that they can implement in organizations, since cybersecurity is currently very important.

Keywords: Threat, Exploit, Hardening, Msfvenom, Payload

INTRODUCCIÓN

En la actualidad muchas de las empresas ya se están preocupando cada día más por la ciberseguridad, por tal razón es importante conocer cómo puede aportar a las organizaciones, teniendo en cuenta que ahora el mundo está conectado y al no estar protegidos pueden tener como resultados, ataques como robo de información, ataques a la infraestructura, suplantaciones, malware, ingeniería social, entre otros[1].

De allí surge la necesidad de establecer medidas de seguridad, que ayuden a mitigar y contrarrestar las posibles amenazas a las que se ven expuestas las organizaciones a diario, por tal razón las funciones que realizan los grupos Red Team, Blue Team y Purple Team son necesarias y muy útiles, su implementación permite tanto la realización de pruebas de penetración como la defensa ante un ataque y aunque los grupos son diferentes, se complementan entre sí.

[1] CISCO. ¿Qué es la ciberseguridad? Cisco [Sitio web]. [Consultado el 3, abril, 2024]. Disponible en Internet: <https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~tipos-de-amenazas>.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Analizar las labores de un equipo Red Team & Blue Team de una organización teniendo en cuenta el marco de los criterios éticos, legales y capacidades técnicas.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar la ley 1273 de 2009 y ley 1581 de 2012.

- Exponer a partir del uso de metodologías y técnicas de intrusión las vulnerabilidades que puede tener un sistema informático.

- Realizar estrategias de contención de ataques, por medio del análisis de vulnerabilidades y riesgos de una infraestructura.

2 LEY 1273 DE 2009 Y LEY 1581 DE 2012

Por medio de la ley 1273 de 2009, se sancionan aquellos delitos que vayan en contra de los pilares de la seguridad de la información, en donde se tipifican 9 delitos, descritos en la tabla 1.

Tabla 1. Ley 1273 de 2009

ARTÍCULO	TIPIFICACIÓN	MODALIDAD	MODO
269 A	Acceso abusivo a un sistema informático	Acceso físico o remoto	La manera como pueden acceder abusivamente a los sistemas puede ser, Phishing, ingeniería social, explotación de vulnerabilidades.
269 B	Obstaculización ilegítima de sistema informático o red de telecomunicación	Impedir u obstaculizar un sistema de información	Se puede presentar ataques Dos, DDos, ransomware
269 C	Interceptación de datos informáticos	Interceptación de datos personales o impersonales	Pueden presentarse ataques con trojanos, Ataque MitB Man in the browser o middle

269 D	Daño Informático	Daño informático a nivel lógico o físico.	Se puede dar por daño en la infraestructura, software malicioso o defacement.
269 E	Uso de software malicioso	Desarrollo, uso o distribución software.	Software malicioso
269 F	Violación de datos personales	Vulneración de los pilares de la seguridad de la información.	Utilización de ingeniería social, phishing, Vishing.
269 G	Suplantación de sitios web para capturar datos personales	Se presenta la implementación, comercialización o desarrollo web	Utilización de ingeniería social, explotación de vulnerabilidades, phishing.
269 H	Circunstancias de agravación punitiva	Obteniendo acceso a un sistema informático o redes u aprovechándose de la confianza de la persona que tiene acceso a la información.	Ingeniería social

269 I	Hurto por medios informáticos y semejantes	Obtener un bien superando medidas de seguridad o suplantando un usuario.	Se puede presentas SIM SWAP, Software malicioso e ingeniería social.
269 J	Transferencia no Consentida de Activos	Manipulación informática que llega a la transferencia no consentida.	Utilización de ingeniería social, explotación de vulnerabilidades, phishing.

Fuente: SECRETARÍA GENERAL DEL SENADO. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. SECRETARÍA GENERAL DEL SENADO [Sitio web]. (31, diciembre, 2023). [Consultado el 15, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>.

La ley 1581 DE 2012, tiene como objeto el derecho constitucional que tiene toda persona a conocer, actualizar y modificar la información que se encuentra relacionada en cualquier base de datos, en donde se pueda hacer uso de la información allí contenida. En la tabla 2 se dan a conocer los aspectos más importantes de la ley.

Tabla 2. Ley 1581 de 2012

PRINCIPIOS RECTORES	Legalidad en el tratamiento de datos	Actividad reglamentada, que se debe sujetar a lo que esta ley dispone.
	De finalidad	Se tiene una finalidad legitima que vaya en concordancia con la ley y la constitución.
	De libertad	Los datos solo se pueden divulgar u obtener con el conocimiento expreso del dueño de los datos.
	Veracidad o calidad	Toda la información que este sujeta a tratamiento debe ser veraz, clara , completa y exacta y se prohíbe que se de tratamiento de datos incompletos, errados o parciales.
	Transparencia	Se debe garantizar el derecho del titular a obtener de quien realice el tratamiento información acerca de la existencia de los datos.

	Acceso o circulación restringida	Los limites se derivan según la naturaleza de los datos, el tratamiento solo se podrá realizar por personas autorizadas por el titular de los datos.
	Seguridad	Se deberá asegurar que el tratamiento de los datos se realice con las medidas técnicas, administrativas y humanas.
	Confidencialidad	Aquellas personas que no tengan naturaleza de público están en la obligación de garantizar la reserva de la información.
CATEGORIA ESPECIAL DE DATOS	Datos sensibles	Conociéndose como datos sensibles aquellos que afectan la intimidad del titular, en datos sensibles se pueden relacionar los siguientes: - Origen racial o étnico - Preferencia política - Religión - Organización social - Datos de salud - Vida sexual - Datos biométricos
	Tratamiento de datos sensibles (no se	Titular da su autorización expresa, teniendo en cuenta

	prohíben en los siguientes casos)	aquellos que no se requiere autorización por ley.
		Cuando el titular se encuentra en condición de discapacidad y el tratamiento se requiere para salvaguardar el interés vital de la persona.
		Se realice el tratamiento en actividades legitimas
		Cuando se necesitan en virtud del reconocimiento o defensa de algún derecho en proceso judicial.
		Cuando se necesite para estadísticas o finalidad histórica.
DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS.	Derechos de los titulares	El Titular puede tener acceso a su información y así actualizar, modificar o eliminar lo datos.
		El titular puede solicitar la autorización que dio para el tratamiento de sus datos.
		El titular debe ser informado previa solicitud, sobre el uso de sus datos.
		El titular puede realizar una queja ante la superintendencia de industria y comercio, por fallas en la disposición de esta ley.

		Retirar la autorización del tratamiento si se vulnera o no se respeten los derechos, garantías o principios constitucionales.
	Autorización del titular	El tratamiento requiere la autorización informada y previa del titular, en donde se pueda posteriormente consultar.
	Cuando no es necesaria la autorización	Se requiere por una entidad publica
		Datos son públicos
		En casos de urgencia medica
		Autorizado por ley
		Datos que son relacionados con el registro civil de las personas
	Suministro de la información	La información que necesite el titular, esta debe ser de fácil comprensión y sin barreras que impidan su lectura
	Deber de informar al titular el responsable del tratamiento	Debe ser de forma clara
		El tratamiento al cual se someterá sus datos.
		Carácter facultativo
		Derechos como titular
		Los datos como: dirección, teléfono e identificación del responsable del tratamiento.
		Titulares, representantes legales

	Personas a quienes se les suministra la información	
		Entidades públicas o administrativas según su función legal u orden judicial.
PROCEDIMIENTOS	Consultas	El titular o persona a cargo puede solicitar consultar la información que se encuentre en cualquier base de datos y el responsable del tratamiento contará con 10 días hábiles o si se presenta algún inconveniente tendrá un máximo de 5 días más hábiles.
	Reclamos	El titular podrá realizar reclamo ante el responsable del tratamiento, describiendo los hechos y los datos a los que haya lugar, el reclamo será atendido 15 días hábiles contados al día siguiente de recibido el reclamo.
	Requisito de procedibilidad	Se podrá levantar queja ante la superintendencia de industria y comercio después de agotado el tiempo de solicitud o reclamo al responsable del tratamiento.
MECANISMOS DE VIGILANCIA Y SANCIÓN.	Autoridad de protección de datos	La superintendencia de industria y comercio a través de una de la delegatura realizaran la

		vigilancia para garantizar la protección de datos personales.
	Sanciones	Multas de carácter institucional o personal, de hasta 2.000 salarios mínimos LV.
		Suspensión de las actividades relacionadas con el tratamiento hasta por 6 meses.
		Cierre temporal, si después de la sanción no hubieren tomado las medidas y mecanismo indicados por la superintendencia.
		Cierre inmediato y definitivo en cuanto a la operación que trabaje con el tratamiento de datos sensibles.
	Criterios para graduar las sanciones	El grado de peligro o daño
		Beneficio económico
		Reincidencia
		Negativa o resistencia por la investigación de la superintendencia.
		Desacato a cumplir con las normas que establece la superintendencia.

Fuente: --------. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. SECRETARÍA GENERAL DEL SENADO [Sitio web]. (31, diciembre, 2023). [Consultado el 17, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html>.

3 EL PENTESTING

Se basa en realizar ataques en diferentes sistemas o entornos, con el fin de encontrar falencias y vulnerabilidades, con la finalidad de prevenir las fallas que estas podrían ocurrir, a continuación, se relacionaran las etapas de un pentesting[2]:

3.1 RECONOCIMIENTO

Con esta etapa se recolecta toda la información pública acerca del objetivo, teniendo un reconocimiento activo o pasivo

- Reconocimiento Pasivo o también llamado footprinting, no deja ningún rastro cuando recoge información sobre el objetivo, reuniendo datos y no es necesario interactuar directamente con él.
- Reconocimiento Activo o también llamado fingerprinting: Deja algún rastro digital, ya que interactúa con el objeto que está analizando y requiere de permisos para realizar el análisis.

3.2 ESCANEO

Después de realizado el reconocimiento, se realiza un análisis de vulnerabilidades. una de las herramientas que se puede utilizar es Nmap, el cual se utiliza con la autorización del sistema que se está escaneando.

[2] KEEPCODING. Fases de un pentest | KeepCoding Bootcamps. KeepCoding Bootcamps [Sitio web]. (28, julio, 2023). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/>.

3.3 OBTENCIÓN DE ESCANEO

Una vez se obtiene la lista de vulnerabilidades encontradas, un hacker ético debe validar los tipos de exploit que existen para acceder a los sistemas.

3.4 MANTENIMIENTO DEL ACCESO

Esta etapa se encarga de establecer persistencia en el sistema, conociéndose como fase de postexplotación y en donde se pretenden realizar una escalada de privilegios y probar un ataque real de manera controlada.

3.5 BORRADO DE HUELLAS

Después de realizar el ataque simulado, se debe eliminar cualquier evidencia que pueda delatar el atacante, es lo que normalmente realiza un hacker malicioso y se le llama digital footprint.

3.6 ELABORACIÓN DEL REPORTE

Este paso es uno de los más importantes, ya que con el informe que se realiza y que debe ser bastante minucioso, se deben comunicar los hallazgos y amenazas que se encontraron en el sistema, para ello los auditores deben saber expresar correctamente la información, ya que serán una pieza clave para el grupo Blue Team.

4 FOOTPRINTING

Es la primera opción que se tiene para recoger información sobre la red o el hardware, es un procedimiento de exploración en donde se debe recopilar toda la información posible, hay dos tipos de footprinting[3]:

Huella activa: es cuando se realiza una huella al colocarse en contacto con la máquina, también cuando se comparte información, completar formularios en línea y también cuando se aceptan cookies en el navegador.

Huella pasiva: la impresión pasiva es cuando se obtiene información del sistema ubicado remotamente, el usuario no se da cuenta al ser un proceso oculto.

4.1 HERRAMIENTAS PARA REALIZAR FOOTPRINTING

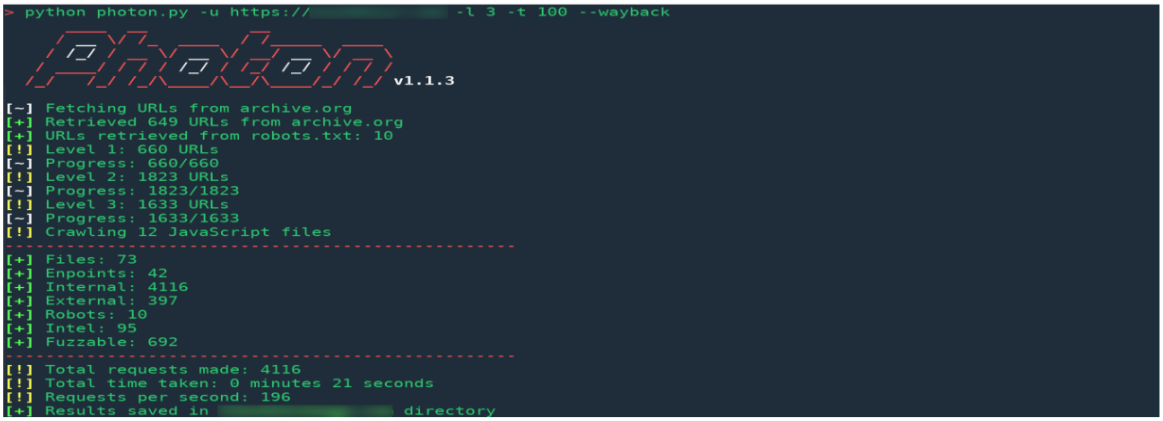
PHOTON: Esta herramienta es muy útil para las técnicas OSINT, esta escrito en Python y disponible en Github, esta herramienta puede extraer información tal como: urls, correos, redes sociales, claves, archivos JavaScript,

Algunas de las características de Photon son[4]:

- Flexible
- Gestión inteligente de procesos
- Complementos
- Se puede inicializar utilizando una imagen Docker
- Actualizaciones frecuentes

[3] CIBERSEG1922. Footprinting y fingerprinting | ciberseguridad. Ciberseguridad [Sitio web]. (9, diciembre, 2019). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://ciberseguridad.com/amenzas/footprinting-fingerprinting/>.
[4] GITHUB. GitHub - s0md3v/photon: incredibly fast crawler designed for OSINT. GitHub [Sitio web]. [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://github.com/s0md3v/Photon>.

Figura 1. Photon



Fuente: GITHUB. GitHub - s0md3v/photon: incredibly fast crawler designed for OSINT. GitHub [Sitio web]. [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://github.com/s0md3v/Photon>.

RECON-NG: es un marco para el reconocimiento web,escrito en Python. tiene módulos independientes, interacción con bases de datos, funciones de conveniencia integradas, ayuda interactiva y finalización de comandos, Recon-ng proporciona un entorno poderoso en el que se puede realizar un reconocimiento basado en web de código abierto de manera rápida y exhaustiva.

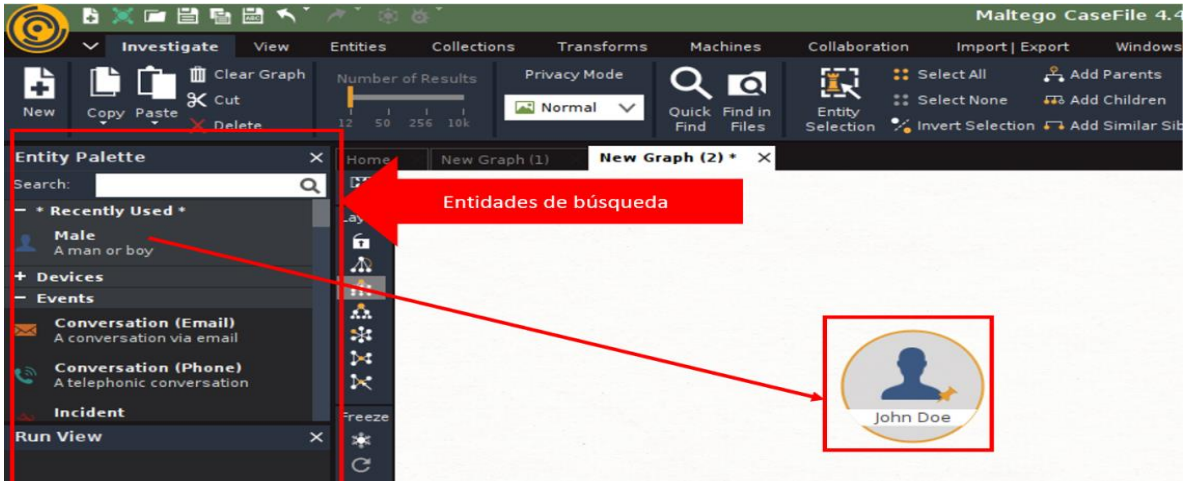
Figura 2. Recon-NG

Fuente: KALI LINUX. Recon-ng | kali linux tools. Kali Linux [Sitio web]. (16, febrero, 2024). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://www.kali.org/tools/recon-ng/>.

MALTEGO: Es una herramienta que permite encontrar información de personas o empresas, es su versión gratuita la búsqueda es limitada, pero bastante extensa, Maltego recolecta información como[5]:

- Red
- Dominio
- Correo electrónico
- Redes sociales
- Malware

Figura 3. Maltego



Fuente: GONZÁLEZ, Sol. Maltego, la herramienta que te muestra qué tan expuesto estás en Internet. Award-winning news, views, and insight from the ESET security community [Sitio web]. (11, mayo, 2023). [Consultado el 18, febrero, 2024]. Disponible en Internet: <https://www.welivesecurity.com/la-es/2023/05/11/maltego-herramienta-muestra-tan-expuesto-estas-internet/>.

[5] GONZÁLEZ, Sol. Maltego, la herramienta que te muestra qué tan expuesto estás en Internet. Award-winning news, views, and insight from the ESET security community [Sitio web]. (11, mayo, 2023). [Consultado el 18, febrero, 2024]. Disponible en Internet: <https://www.welivesecurity.com/la-es/2023/05/11/maltego-herramienta-muestra-tan-expuesto-estas-internet/>.

5 METASPLOIT

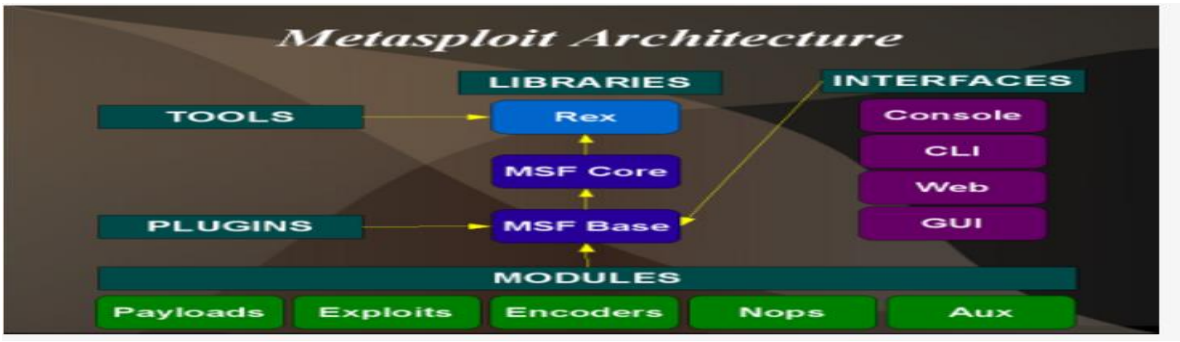
Es un marco de pruebas de penetración, buscando simplificar la verificación de vulnerabilidades.

- Usa bases de datos sobre vulnerabilidades
- Automatiza tareas repetitivas
- Herramienta de aprendizaje
- Principios éticos

Los atacantes siempre están desarrollando nuevos exploits y métodos de ataque, el software de prueba de penetración Metasploit ayuda a utilizar sus propias armas contra ellos. Utilizando una base de datos de exploits en constante crecimiento, puede simular de forma segura ataques reales en su red para capacitar a su equipo de seguridad para detectar y detener los ataques reales.

Los principales componentes de un Metasploit se pueden observar en la Figura 4,

Figura 4 Arquitectura Metasploit



Fuente: H1RD. Introducción a metasploit. H1RD.COM [Sitio web]. (2, agosto, 2017). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://www.h1rd.com/hacking/Introduccion-a-metasploit>.

6 ¿QUÉ ES UN CVE Y SU ESTRUCTURA?

El CVE es un reporte de alguna falla en seguridad informática, la cual se asocia un número de identificación. Mitre corporation es la entidad que se encarga de supervisar los CVE siendo financiado por la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA), que forma parte del Departamento de Seguridad Nacional de Estados Unidos[6].

Los identificadores de CVE son únicos asignados a vulnerabilidades de ciberseguridad conocidos públicamente que afectan al software, el hardware y el firmware.

EL objetivo que tienen los CVE es que las vulnerabilidades que han sido encontradas sean de fácil intercambio.

Estructura de un CVE[7]:

CVE-YYYY-NNNN

- Un nuevo CVE recibe una identificación única
- Fecha de entrada
- Descripción individual
- Campo de referencia

[6] RED HAT. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [Sitio web]. (15, noviembre, 2021). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve>.

[7] --------. ¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes. Ciberseguridad [Sitio web]. (11, octubre, 2021). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/>.

Estados de un CVE:

- Reservado: Este es el estado inicial de un CVE ID.
- Publicado: una CNA ha completado los datos asociados con el ID CVE y ha publicado el registro CVE.
- Rechazado: el ID CVE y el registro CVE asociado ya no deben usarse. Un registro CVE rechazado permanece en la lista CVE para que los usuarios sepan que el ID CVE y el registro CVE no son válidos.

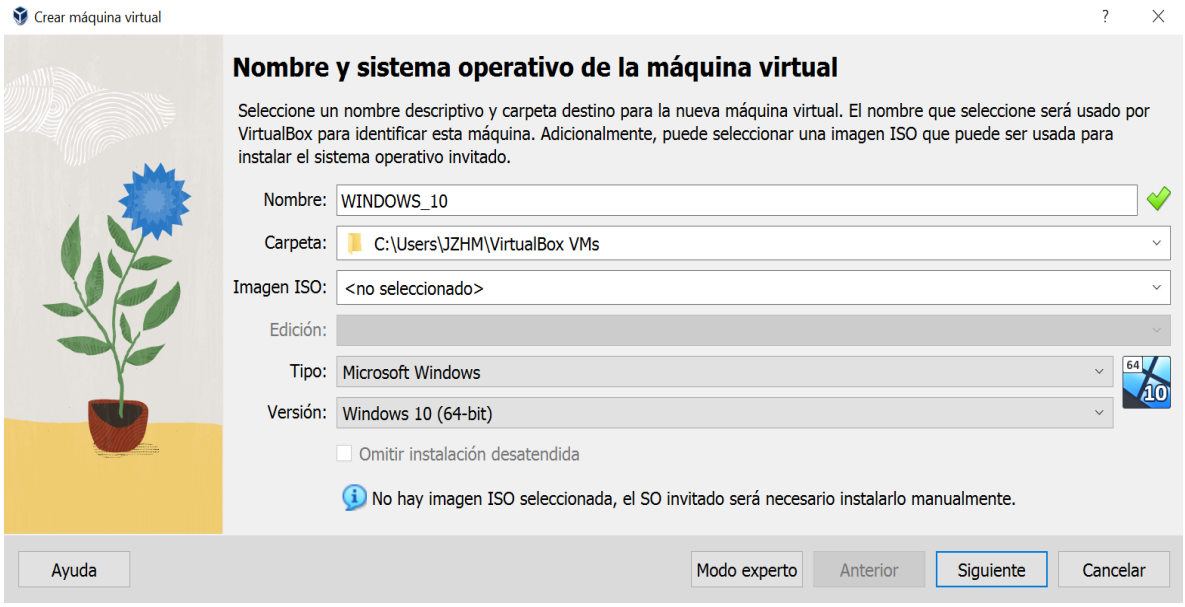
EXPLOITDB[8]: es una Sitio web que reúne bases de datos con los exploit conocidos y pueden ser utilizados de manera gratuita y utilizarlos en las auditorias de seguridad, es creado por la compañía Offensive Security.

La relación que existe entre CVE y EXPLOITDB, es que muchos de los exploit reportados cuentan una identificación CVE, facilitando la correlación entre Exploit y vulnerabilidad.

[8] KEEPCODING. ¿Qué es ExploitDB? | KeepCoding Bootcamps. KeepCoding Bootcamps [Sitio web]. [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-exploitdb/>.

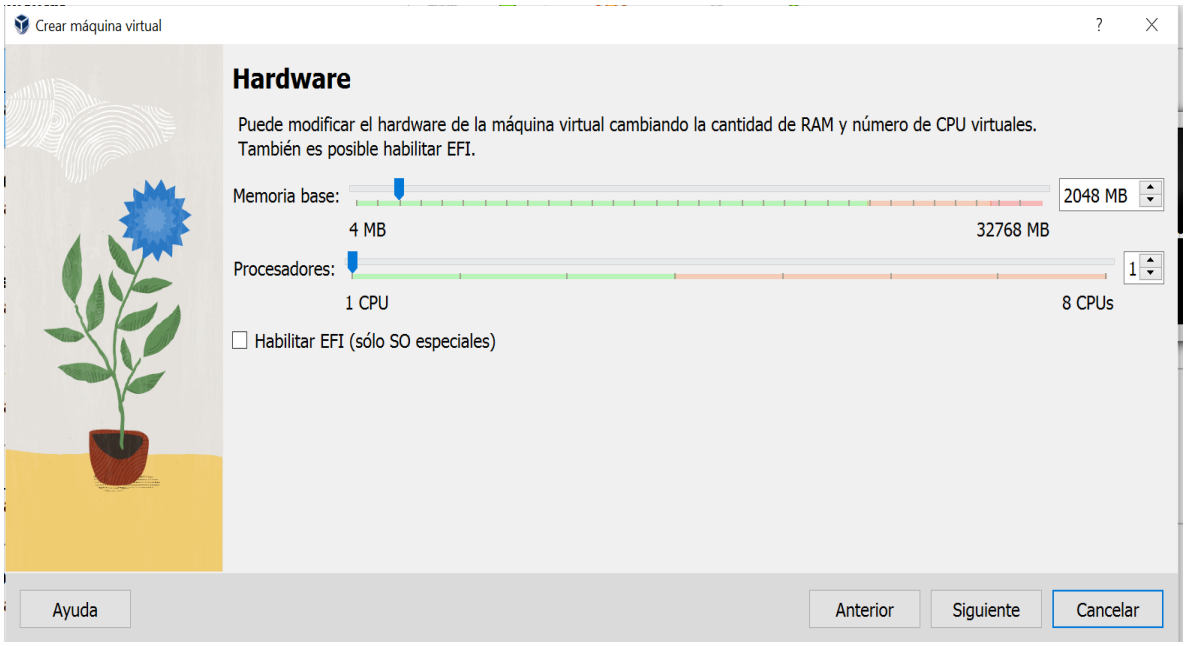
7 BANCO DE TRABAJO

Figura 5. Configuración MV Windows



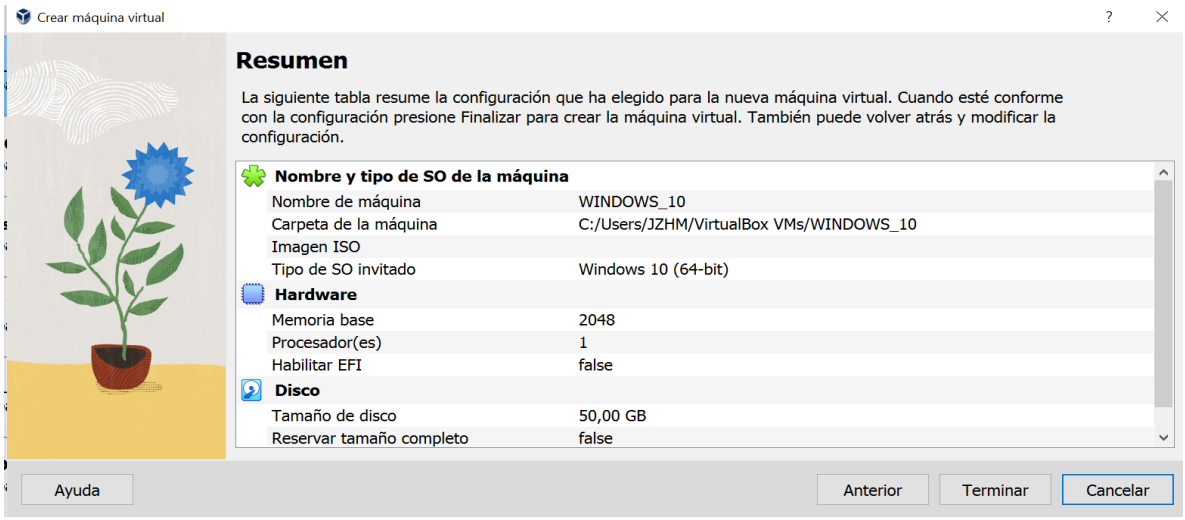
Fuente: Propia

Figura 6. Configuración HW Windows



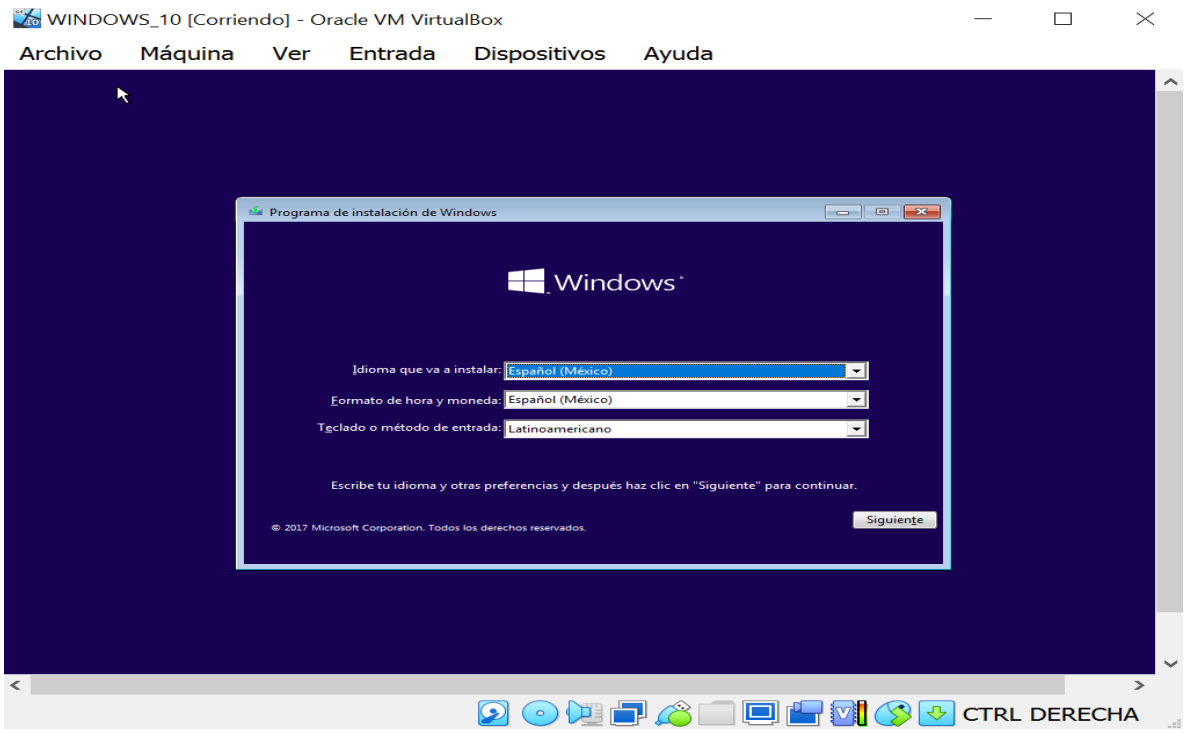
Fuente: Propia

Figura 7. Resumen configuración Windows



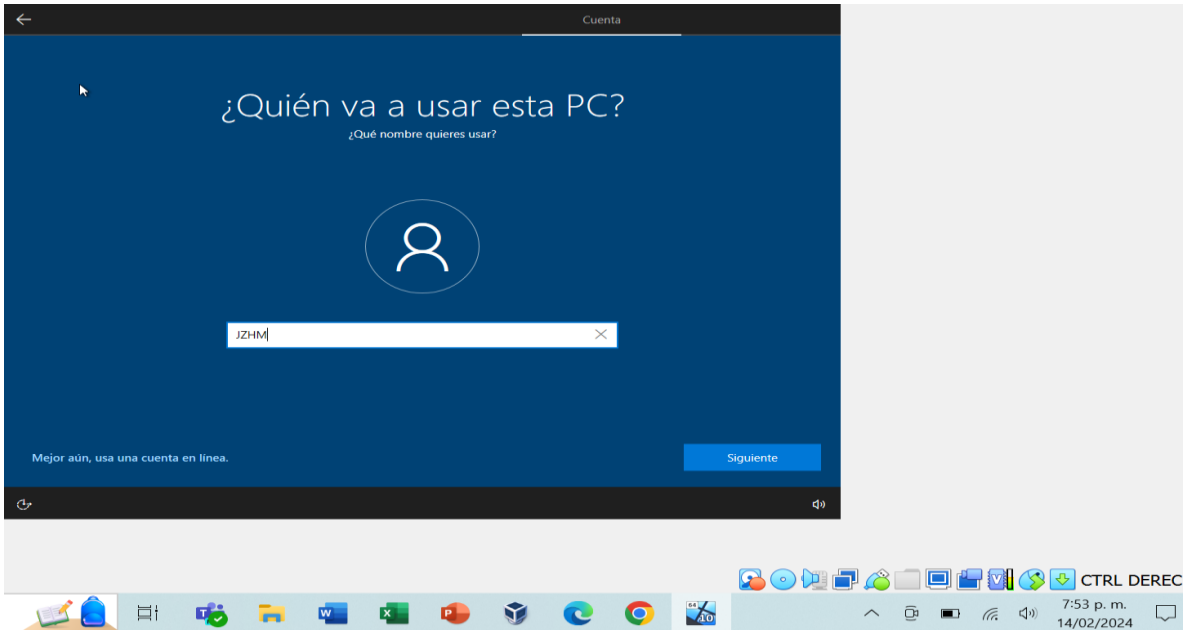
Fuente: Propia

Figura 8. Instalación Windows



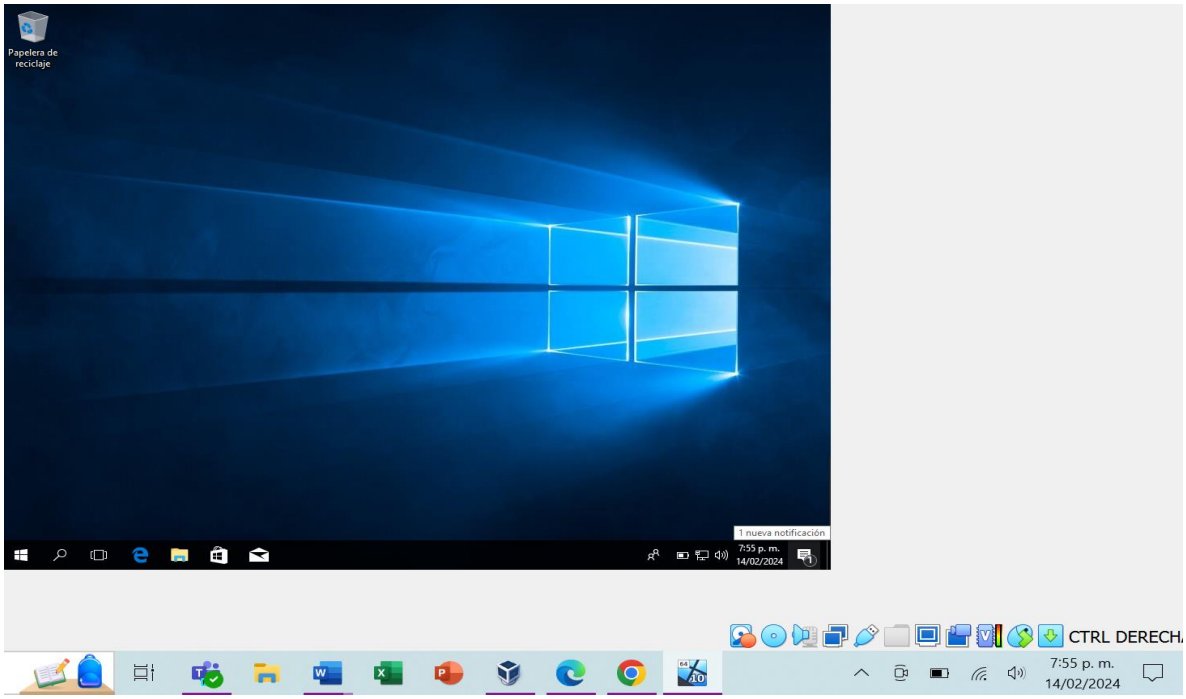
Fuente: Propia

Figura 9. Configuración usuaria Windows



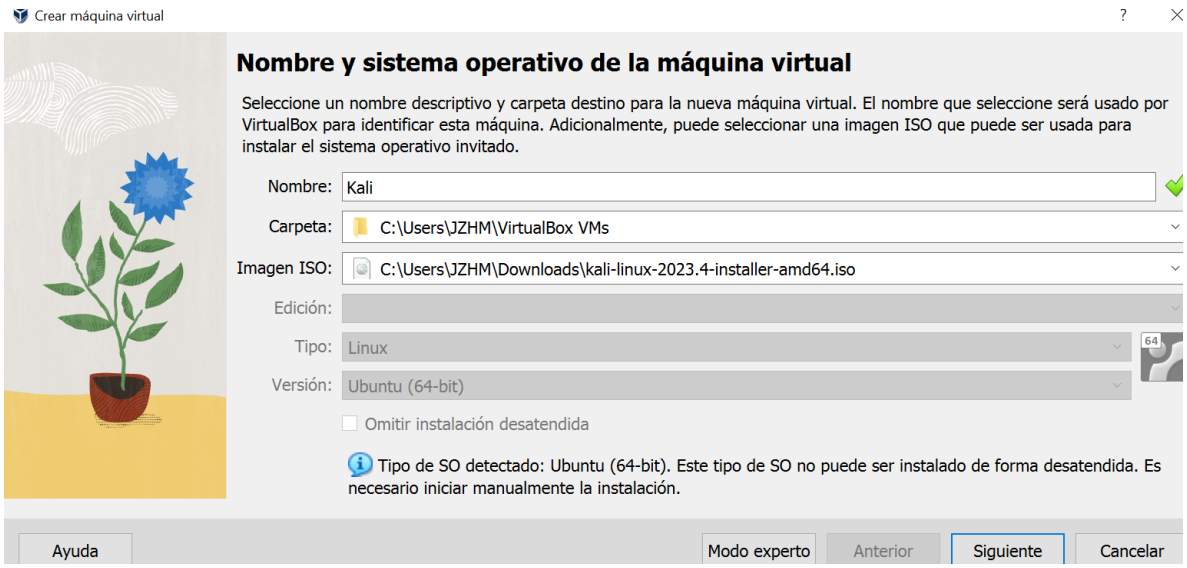
Fuente: Propia

Figura 10. Inicio Windows



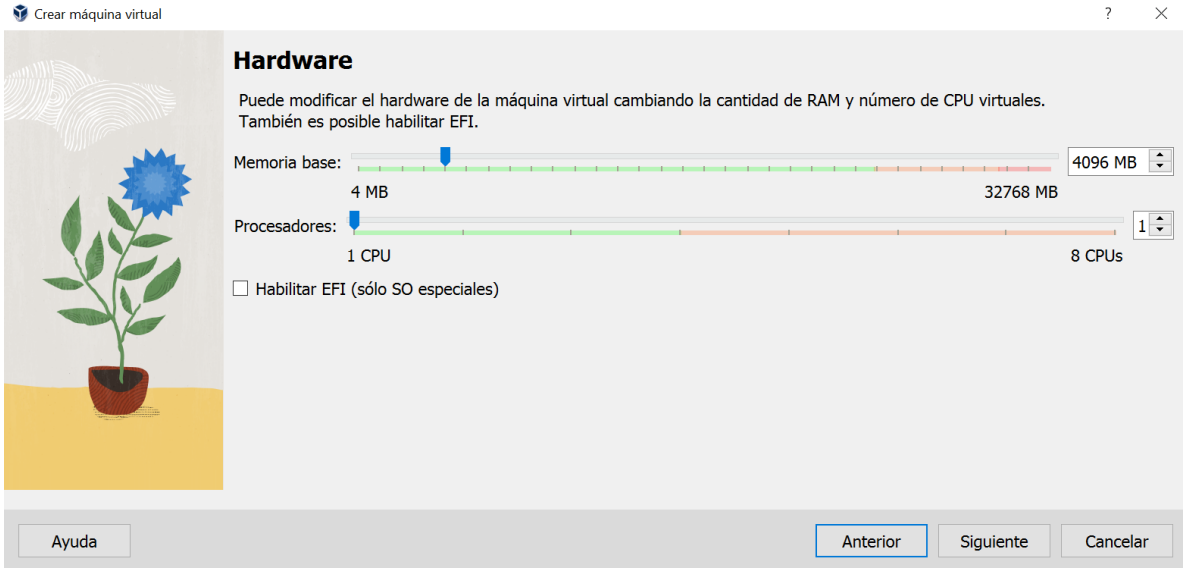
Fuente: Propia

Figura 11 Configuración MV Kali



Fuente: Propia

Figura 12 Configuración HW Kali

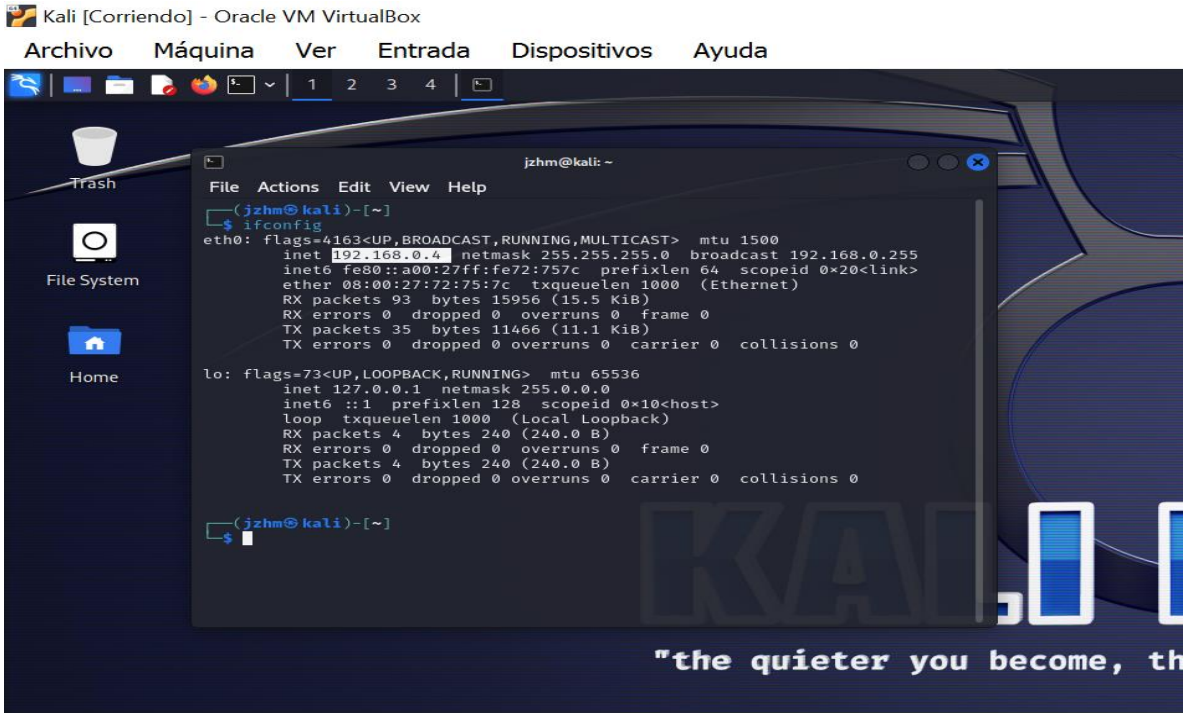


Fuente: Propia

Figura 13. Instalando Kali

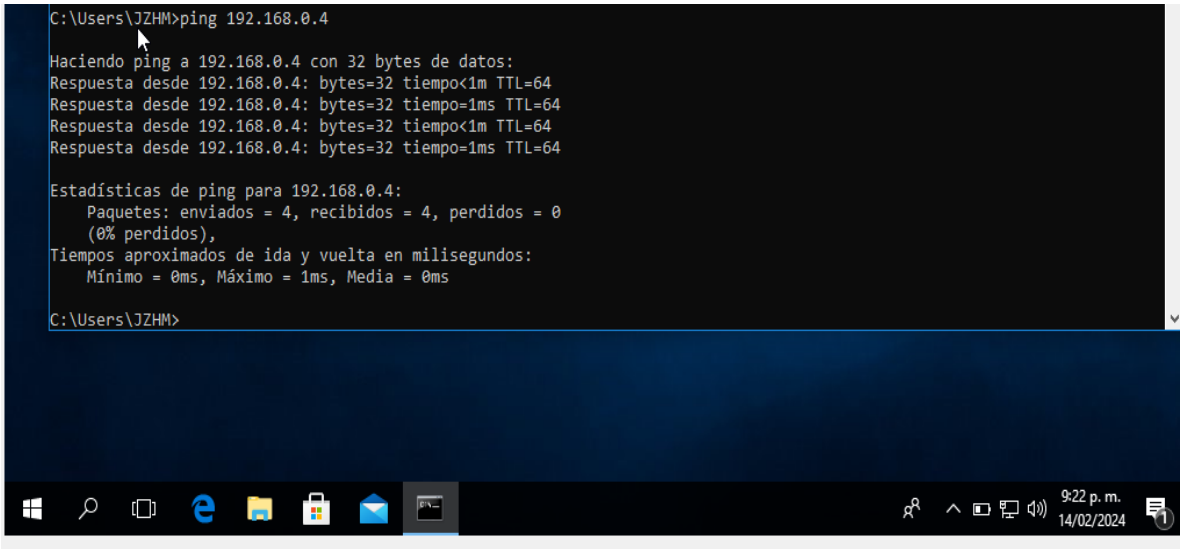
Fuente: Propia

Figura 14. IP Kali



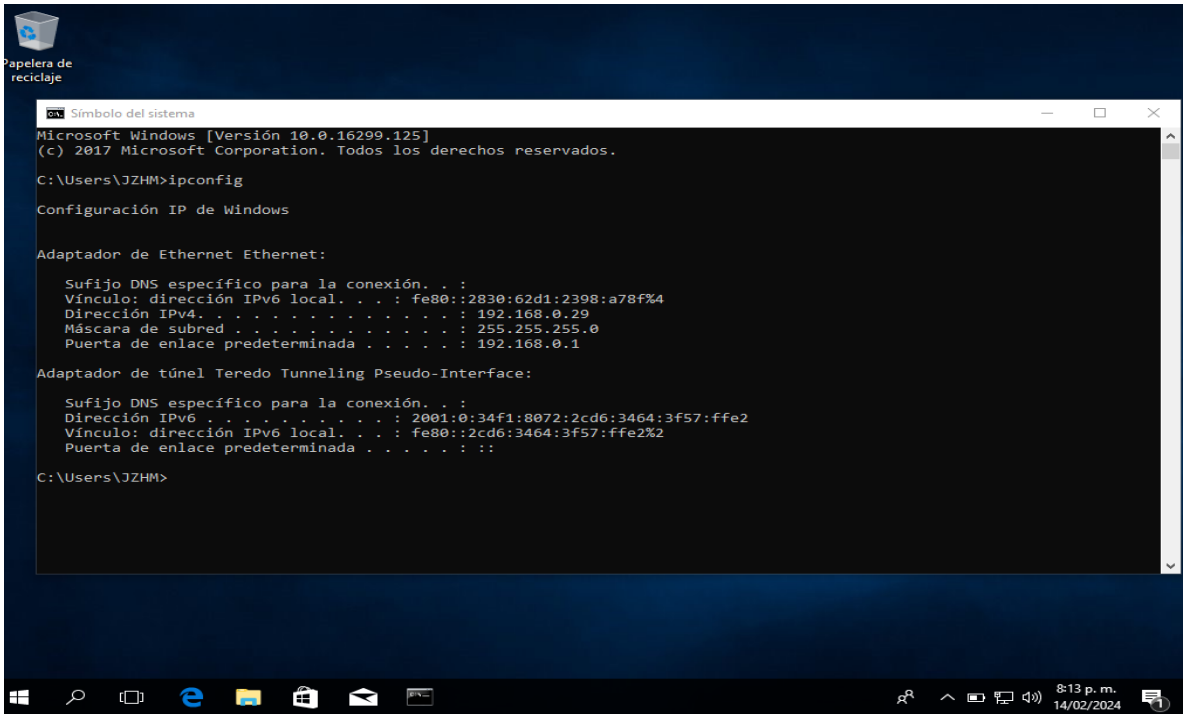
Fuente: Propia

Figura 15. Ping desde Windows a Kali



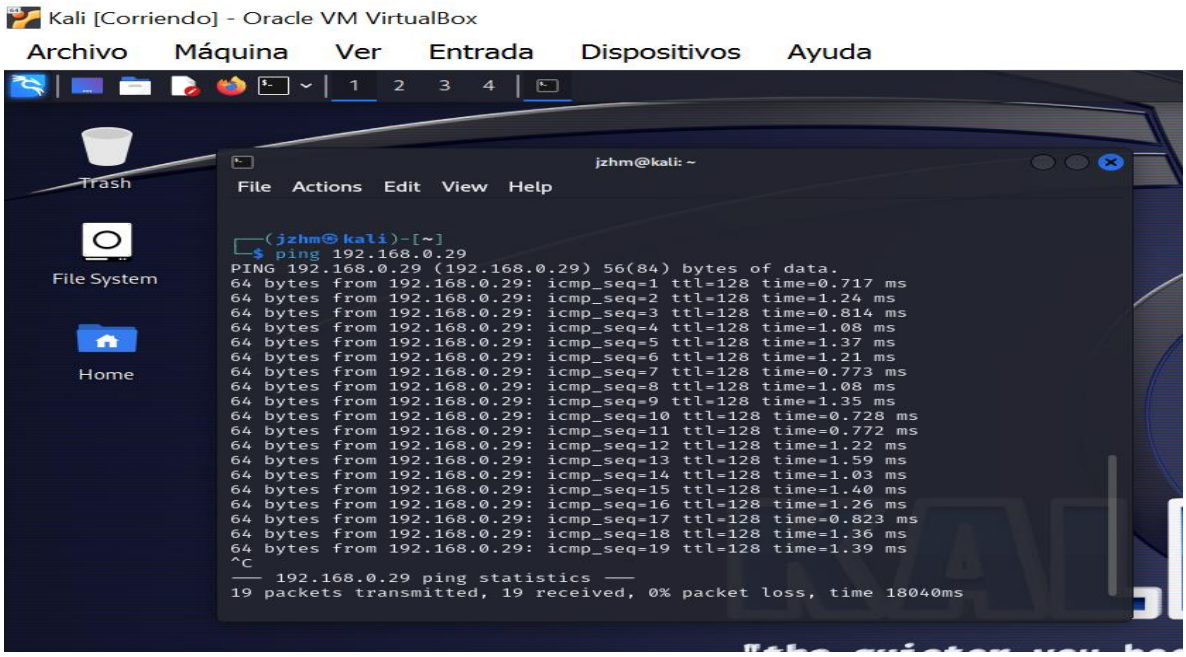
Fuente: Propia

Figura 16. IP Windows



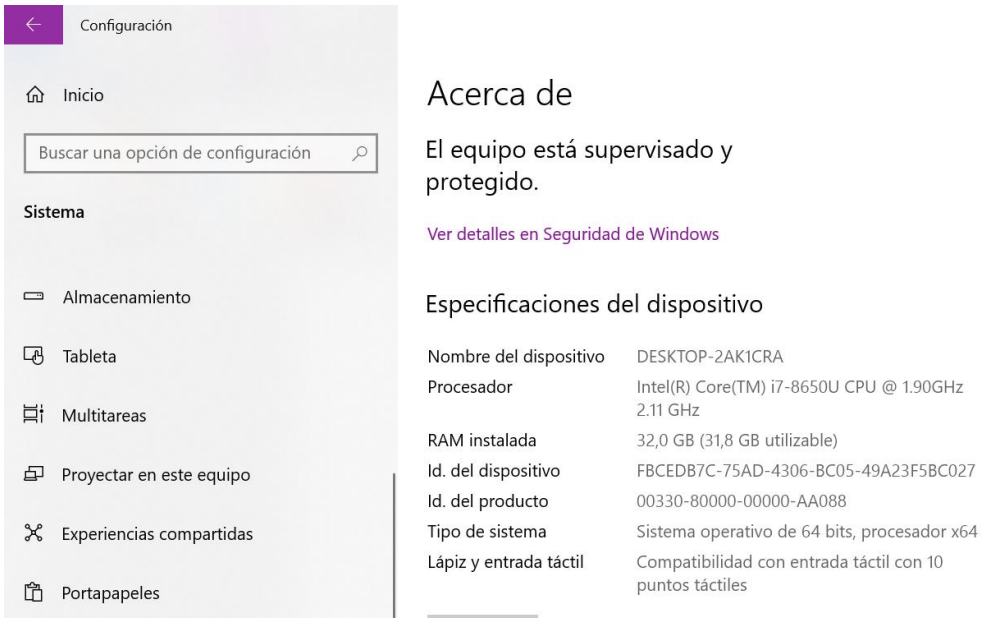
Fuente: Propia

Figura 17. Ping desde Kali a Windows



Fuente: Propia

Figura 18. Recursos de HW Maquina anfitriona



Fuente: Propia

8 PROCESOS ILEGALES ANEXO 2 Y ANEXO 3

De acuerdo al anexo 2, el párrafo dos se torna ilegal ya que el acuerdo de confidencialidad, fue realizado por un ex empleado y además por que no salió de la empresa de una forma positiva, si no por el contrario, fue despedido por procesos ilícitos, adicional el área de recursos humanos no tuvo en cuenta ninguna validación al acuerdo de confidencialidad.

Se realiza validación del acuerdo de confidencialidad y se encontró las siguientes inconsistencias:

Cláusula Primera, “sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.”

Aquí nos está indicando que la empresa realiza procesos ilegales y lo que pretenden, es que los empleados no ejerzan de una manera honesta su labor, si no que se queden callados ante cualquier eventualidad, aunque bien es cierto que la confidencialidad debe existir por el tipo de información que se puede manejar en la empresa, como datos sensibles, no se puede no divulgar los actos ilegales.

Clausula Segunda, datos secretos como “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”.

La empresa está diciendo abiertamente que interceptan información de una forma ilegal, lo que no está permitido según la ley 1273 de 2009[9]

[9] FISCALÍA GENERAL DE LA NACIÓN. Cartilla metodológica de atención de delitos informáticos. Fiscalia General de la Nación [Sitio web]. (21, septiembre, 2023). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf>.

Clausula Cuarta numeral 3, “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.”

Nuevamente nos muestran que la empresa realiza actividades que no están permitidas dentro de las leyes colombianas.

Clausula Cuarta numeral 4, “Responder por el mal uso que le den sus representantes a la información confidencial.”

No es justo que la responsabilidad recaiga en un solo empleado, ya que el tratamiento de la información se da por varias personas.

Clausula Cuarta numeral 5, “Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.”

Con esta cláusula la empresa está tratando de librarse de culpas y que el empleado quede en frente ante cualquier culpabilidad encontrada por las autoridades.

Clausula Cuarta numeral 6,” la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse.”

Con la cláusula 4, numeral 3, 4,5 y 6 están impidiendo que se realice denuncia, si se encuentran irregularidades, por lo tanto, se podría infringir el código de ética del COPNIA, también que toda la responsabilidad recaiga en el empleado y que la empresa quede libre de culpas.

Clausula Octava, “En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.”

Este tipo de inconsistencias denota que la empresa realiza actividades ilícitas y que quiere que la responsabilidad recaiga en los empleados que firmen este acuerdo de confidencialidad.

9 LEY QUE SE PODRIA ESTAR VIOLANDO EN EL ANEXO 2 Y 3

Una vez se identificaron las inconsistencias en el acuerdo de confidencialidad, se puede relacionar con las siguientes leyes, las cuales posiblemente se estarían violando, Ley 1273 de 2009[10] y Ley 581 de 2012[11] :

- Ley 1273 de 2009 - artículo 269 A: Ya que se está accediendo a información o sistemas informáticos de una manera abusiva.

- Ley 1273 de 2009 - articulo 269 B: se está accediendo de una forma ilegitima al sistema informático

- Ley 1273 de 2009 - articulo 269 C – Están obteniendo información por medio de chuzadas y formas no adecuadas.

[10] FISCALÍA GENERAL DE LA NACIÓN. Cartilla metodológica de atención de delitos informáticos. Fiscalia General de la Nación [Sitio web]. (21, septiembre, 2023). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf>.

[11] --------. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. SECRETARÍA GENERAL DEL SENADO [Sitio web]. (31, diciembre, 2023). [Consultado el 17, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html>.

- Ley 1273 de 2009 - articulo 269 F - Violación de datos personales

- Ley 1273 de 2009 - articulo 269I - Hurto por medios informáticos y semejantes

- Ley 581 de 2012 – Articulo 4 numeral g – Principio de seguridad

- Ley 581 de 2012 – Articulo 17 numeral n - Articulo 18 numeral b – No están teniendo en cuenta los deberes de las personas que realizan el tratamiento.

10 CÓDIGO DE ÉTICA - COPNIA

Validando el código de ética del COPNIA, se puede tener como un manual de conducta de los ingenieros, en donde se especifica las obligaciones, deberes, prohibiciones, inhabilidades e incompatibilidades relacionadas con la ejecución de la profesión, en busca de que los profesionales actúen de manera honesta y con compromiso.

a continuación, se relacionan todos los capítulos y artículos contenidos en el código de conducta del COPNIA, para tener una visión más amplia, de lo que los profesionales deben o no hacer según tabla 3:

Tabla 3. Código de ética del COPNIA

CAPITULO	ARTICULO	DESCRIPCIÓN
I POSTULADOS ÉTICOS DEL EJERCICIO PROFESIONAL.	29	Es un marco de comportamiento de los profesionales, en donde se debe ajustar a las normas establecidas por el código.
	30	Los ingenieros o con títulos afines se denominan profesionales.
II DEBERES Y OBLIGACIONES	31	Se establece todos los deberes que deben tener en cuenta los profesionales. Se debe custodiar información, documentos o bienes que se encuentren a cargo en el desempeño de las funciones. Se deben denunciar todos los delitos que vayan en contra con este código.
	32	Permitir el ejercicio ilegal Solicitar dineros o comisiones por la prestación de sus servicios. Incumplir decisiones del COPNIA
	33	Validar cuidadosamente cada ambiente en el que se vaya a ejercer la profesión.

		No emitir conceptos profesionales, si no se tiene la suficiente información o convencimiento absoluto. Siempre proteger la vida, salud y el patrimonio nacional.
	34	Este artículo en marca las prohibiciones que tienen los profesionales. No se puede aceptar trabajos en los que se violen las leyes vigentes. Contribuir para que se realicen diplomas, actas, tarjeta profesional a personas que no reúnen los requisitos.
	35	Este articulo habla sobre los deberes de los profesionales y la dignidad de la profesión. Respetar todas las disposiciones legales. Atender por el buen prestigio en el ejercicio de la profesión.

	36	Se prohíbe recibir cualquier tipo de beneficios ilegales, tales como comisiones o regalos.
	37	Se relacionan los deberes que tienen los profesionales con sus colegas.
	38	Prohibiciones con respecto a sus colegas. No se puede utilizar archivos, diseños, software, cálculos, etc, sin previa autorización del dueño. No utilizar métodos desleales con los colegas
	39	Deberes con los clientes Mantener reserva con los trabajos que se realizan a un cliente. Atender con diligencia y aptitud los asuntos de sus clientes.
	40	Prohibiciones respecto a los clientes Ofrecer servicios que sean de dudosa o no posible cumplimiento. Aceptar beneficios de terceros

	41	Deberes de los profesionales en un cargo público o privado Se debe actuar de manera imparcial en el momento de fijar o preparar pliegos
	42	Prohibiciones de los profesionales en un cargo público o privado Participar en procesos evaluativos sobre tareas de sus colegas.
	43	Deberes de los profesionales en licitaciones
	44	Prohibiciones de los profesionales en licitaciones
III INHABILIDADES E INCOMPATIBILIDADES DE LOS PROFESIONALES	45	Inhabilidades e incompatibilidades de los profesionales No se puede desempeñar como profesional al mismo tiempo en dos empresas, sin previo consentimiento de las partes. Se puede intervenir como perito cuando estén presentes las inhabilidades de ley.

Fuente: COPNIA. Código de ética | Copnia. Inicio | Copnia [Sitio web]. [Consultado el 23, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

Luego de ver las disposiciones que se encuentran en el código de ética del Copnia[12] y teniendo en cuenta como primer punto mi actuar como persona, se da respuesta a la pregunta:

¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería?

- Por principios éticos no aceptaría firmar el principio de acuerdo y tampoco trabajaría en la empresa, ya que es posible que se dedique a actividades ilícitas.
- En el capítulo 2 articulo 31, se puede observar, que los profesionales debemos custodiar la información como lo indica el numeral b y denunciar todos aquellos delitos que se encuentren, según numeral f
- En el capítulo 2 articulo 34, en dónde en el numeral a mencionan que no se pueden aceptar trabajos que vayan en contra con las disposiciones legales vigentes
- También se puede tener la cancelación de la matricula profesional, ya que se considera una falta gravísima según el numeral e, cometer algún delito que atente contra algún cliente, colega en el ejercicio de la profesión.

[12] COPNIA. Código de ética | Copnia. Inicio | Copnia [Sitio web]. [Consultado el 23, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

11 NOTICIA SOBRE CIBERCRIMEN

El 14 de septiembre de 2023, el periódico el país[13] publico la noticia sobre un hackeo masivo en Colombia, donde las páginas web del ministerio de la salud, la rama judicial, la superintendencia de industria y comercio, entre otras estuvieron caídas y ya era el tercer día del incidente.

El ataque cibernético inicio cuando un software ataco varias máquinas virtuales de IFX, la empresa confirmo que fue un archivo tipo Ransomware, afectando a varias empresas, como también lo estuvieron el ministerio y sistema de salud, en donde los pacientes no pueden pedir citas y los médicos no tenían acceso a las historias clínicas.

Para este caso y validando las leyes, en donde se identifica el delito que se cometió al realizar el hackeo masivo:

- Ley 1273 de 2009, Articulo 269 A
- Ley 1273 de 2009, Articulo 269 B
- Ley 1273 de 2009, Articulo 269 D
- Ley 1273 de 2009, Articulo 269 E
- Ley 1273 de 2009, Articulo 269 F
- Ley 1273 de 2009, Articulo 269 I

[13] OWNBY, Jules. Hackeo masivo en Colombia: “La información de millones de personas está en manos de delincuentes en este momento”. El País América Colombia [Sitio web]. (14, septiembre, 2023). [Consultado el 24, febrero, 2024]. Disponible en Internet: <https://elpais.com/america-colombia/2023-09-14/hackeo-masivo-en-colombia-la-informacion-de-millones-de-personas-esta-en-manos-de-delincuentes-en-este-momento.html>.

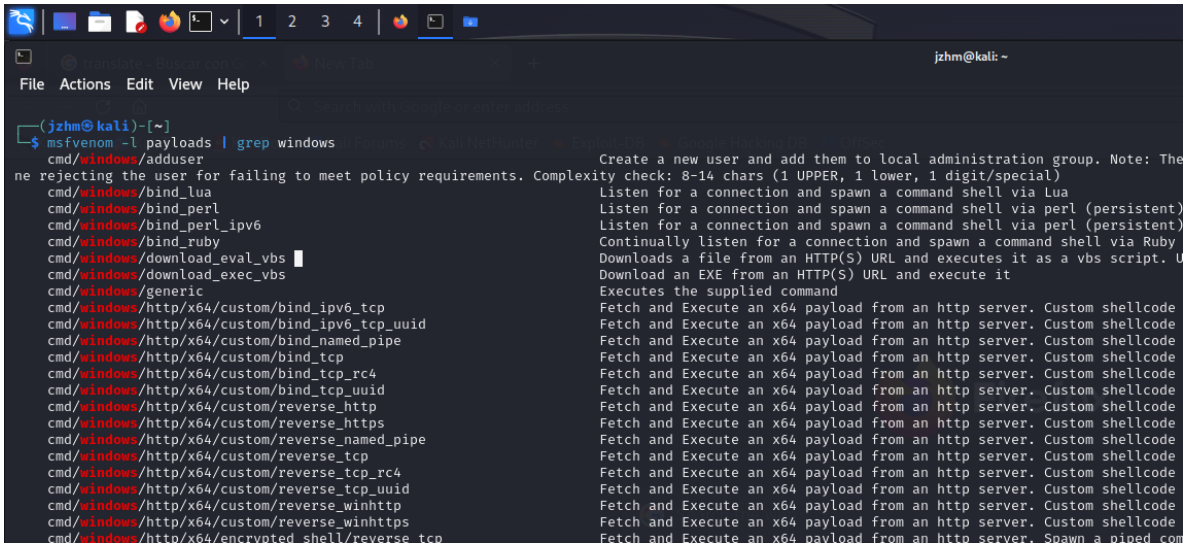
12 HERRAMIENTAS UTILIZADAS EN EL ANEXO 4 – ESCENARIO 3

12.1 MSFVENOM

Utiliza líneas de comandos para la creación de Payloads personalizados, se pueden crear para diferentes arquitecturas y sistemas operativos[14].

Para nuestro ejercicio se utilizó un Payload para Windows, en donde podemos ver las opciones al ejecutar el comando msfvenom -l payloads | grep Windows, como se muestra en la Figura 1.

Figura 19, Payloads en Msfvenom para Windows



Fuente: Propia

[14] GITBOOK. MsfVenom | cheatsheet. Introducción | Cheatsheet [Sitio web]. [Consultado el 15, marzo, 2024]. Disponible en Internet: <https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/explotacion-de-vulnerabilidades/explotacion-en-hosts/msfvenom>.

12.2 PAYLOAD

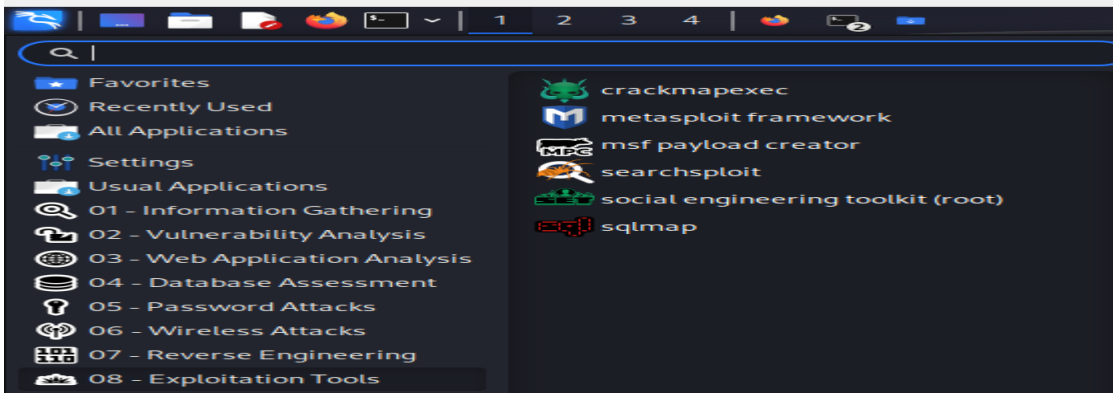
Es un conjunto de instrucciones maliciosas con la finalidad de infiltrarse al equipo de su víctima y conseguir ejecutar tareas, que permitan por ejemplo: el control de la máquina, enviar archivos, ejecutar una botnet.y despliegue de software malicioso, entre otros[15].

Existen dos clases de Payload, directo e inverso, para nuestro ejercicio se utilizó el inverso y para su ejecución se utilizó el framework Metasploit.

12.3 METASPLOIT

Se utiliza para la explotación de vulnerabilidades, aprovechando fallos en los sistemas, también contiene herramientas de postexplotación que permiten la ejecución en la máquina de la víctima[16].

Figura 20. Metasploit



Fuente: Propia

[15] --------. ¿Qué es un payload? | KeepCoding Bootcamps. KeepCoding Bootcamps [Sitio web]. (2, octubre, 2023). [Consultado el 15, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-un-payload/>.

[16] KEEPCODING BOOTCAMPS. 4 herramientas de postexplotación | KeepCoding Bootcamps. KeepCoding Bootcamps [Sitio web]. (23, noviembre, 2023). [Consultado el 15, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/herramientas-de-postexplotacion/>.

Él Mestasploit ya viene preinstalada en Kali, como se observa en la Figura 20.

12.4 METERPRETER

Es una carga útil que permite por medio de una conexión inversa, enviar código a la maquina víctima, los comandos utilizados para nuestro anexo, son los siguientes[17]:

Sysinfo: con este comando se obtiene la información de la máquina.

Ls: lista los archivos que tiene la maquina objetivo

Rm: Elimina el archivo indicado

12.5 NMAP

Es una herramienta muy utilizada para realizar auditorías de seguridad y exploración de la red, permite obtener información de máquinas en una red, sistemas operativos indicando sus versiones, el tipo de cortafuegos que está utilizando y muchas otras características utilies para el reconocimiento de la máquina[18].

[17] CUNHA BARBOSA, Daniel. Metasploit Framework: explotar vulnerabilidades puede ser bastante fácil. Award-winning news, views, and insight from the ESET security community [Sitio web]. (23, octubre, 2023). [Consultado el 15, marzo, 2024]. Disponible en Internet: <https://www.welivesecurity.com/es/recursos-herramientas/metasploit-framework-explotar-vulnerabilidades/>.

[18] NMAP.ORG. Guía de referencia de Nmap (Página de manual). Nmap: the Network Mapper - Free Security Scanner [Sitio web]. [Consultado el 16, marzo, 2024]. Disponible en Internet: <https://nmap.org/man/es/index.html#man-description>.

Las salidas que proporciona Nmap es un listado con los objetivos que se han analizado, para la cual en nuestra actividad nos fue de utilidad, la lista de puertos, en donde podemos identificar es estado como open, filtered, closed o unfiltered.

13 IDENTIFICACIÓN DE FALLO

Al realizar el análisis del problema expuesto por el administrador del equipo, se encontraron datos muy importantes que se deben tener en cuenta en la realización y utilización de las herramientas adecuadas, que nos lleven a identificar lo sucedido, los puntos claves son:

- Administrador indica la eliminación de archivo.
- Envío de archivo sospechoso que el administrador procede a descargar y a ejecutar en la máquina.
- Sistemas de seguridad deshabilitados.

14 HERRAMIENTA UTILIZADA PARA LA IDENTIFICACIÓN DEL FALLO

La herramienta que se utilizó para realizar el escaneo de la máquina, fue Nmap en donde se encontró el siguiente hallazgo:

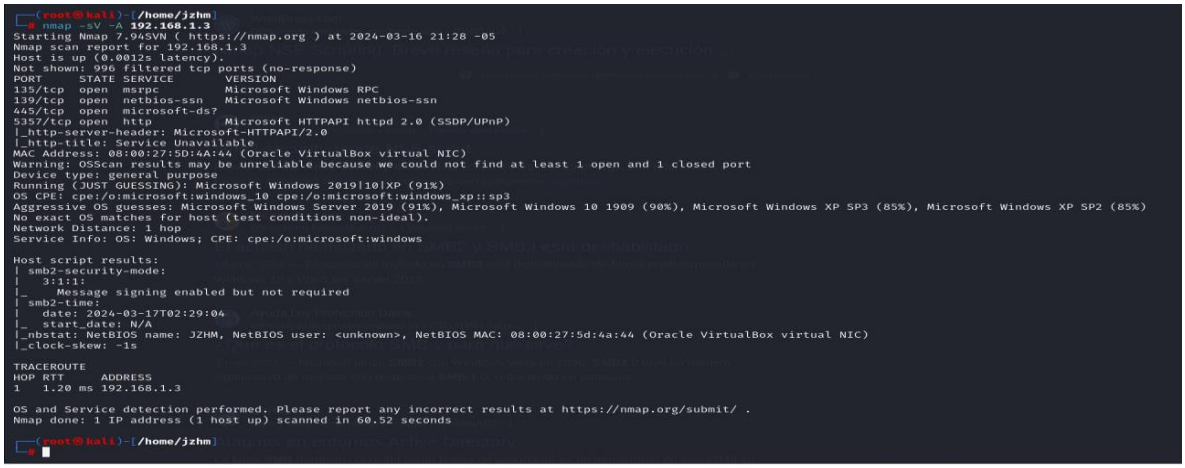
Detección de puertos habilitados

Figura 21. Escaneo Nmap

Fuente: Propia

Detección de versión y sistema operativo

Figura 22. Detección versión y SO



Fuente: Propia

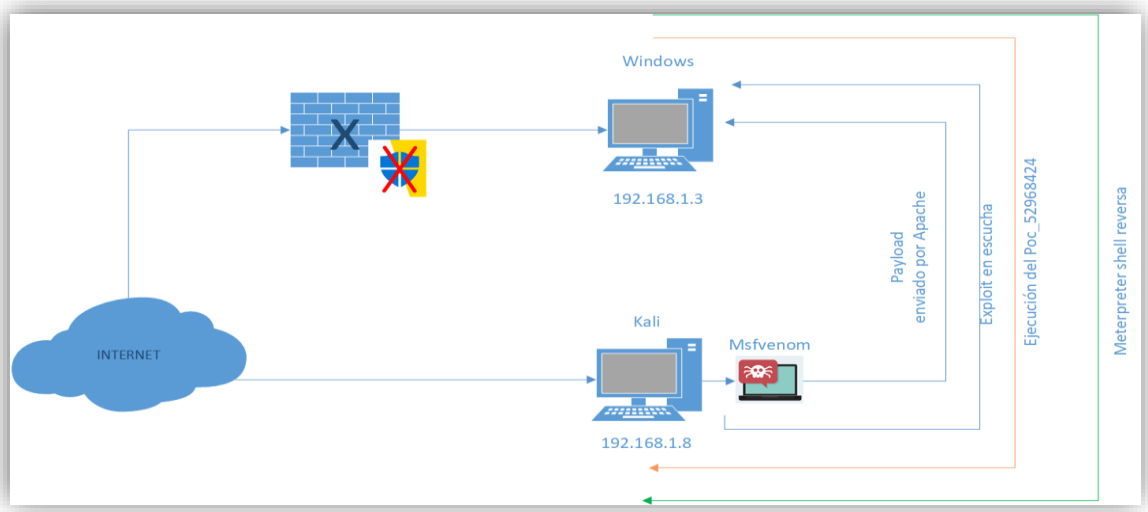
15 DIAGRAMA EXPLOTACIÓN DEL ATAQUE

En la figura 5. se evidencia el diagrama del ataque, teniendo cuenta los siguientes pasos realizados:

Tenemos dos máquinas, una Kali que es por medio donde se va a realizar el ataque y una maquina Windows que va a ser nuestro objetivo.

Por medio de Msfvenom se creó un Payload para enviar a la maquina Windows
Después se envió por medio del servidor apache para que el usuario descargara el archivo.
Luego se abre un exploit para quedar a la escucha y que el usuario de la maquina Windows ejecute el archivo.
Una vez ejecutado el archivo, el exploit ejecutara el meterpreter por medio de una Shell reversa.
Se evidenciará el acceso de la maquina Kali hacía la maquina Windows

Figura 23. Diagrama ataque

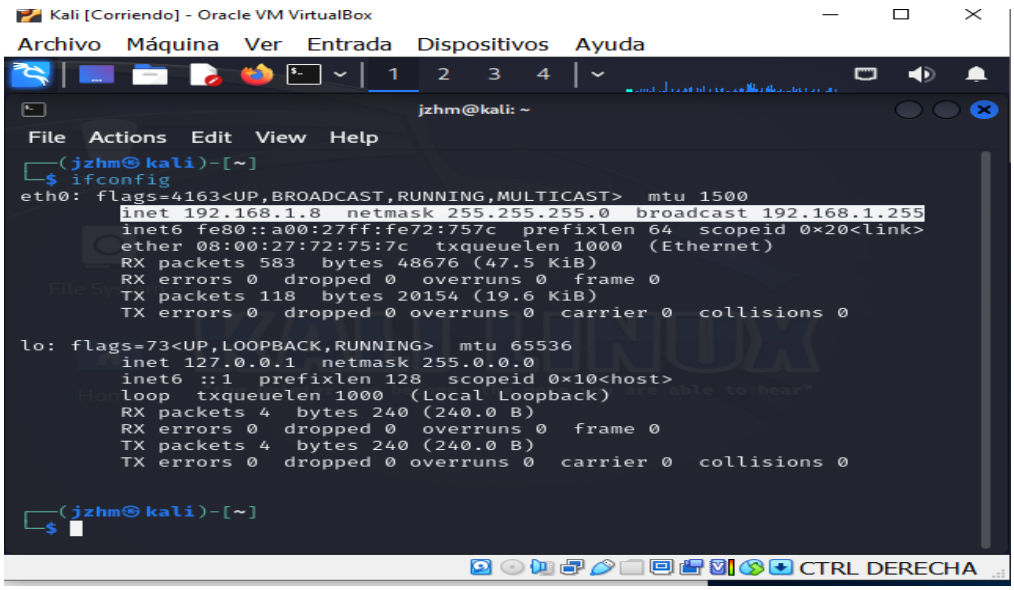


Fuente: Propia

16 DESARROLLO DEL ANEXO 4 - ESCENARIO 3

Se realiza la identificación de la IP de nuestra maquina Kali

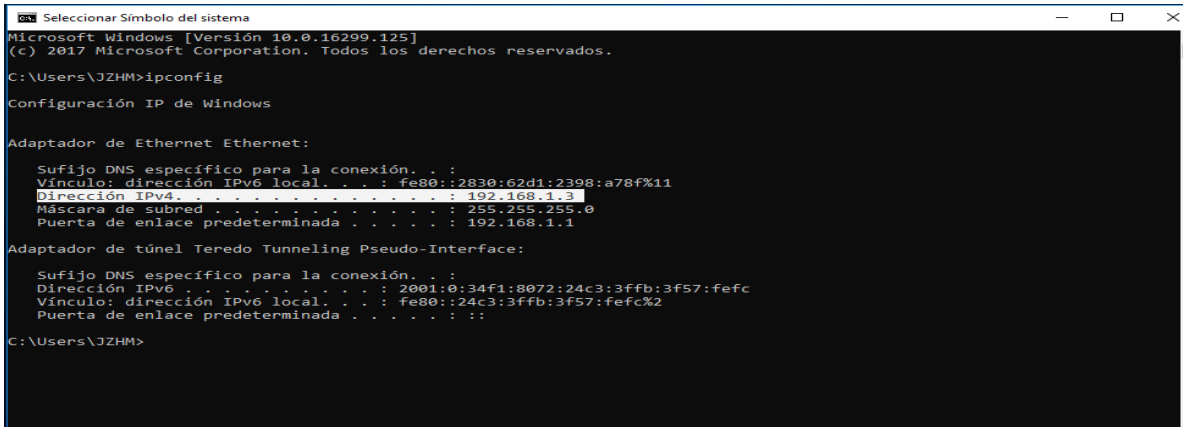
Figura 24. IP Kali



Fuente: Propia

Se realiza la identificación de la IP de nuestra maquina Windows

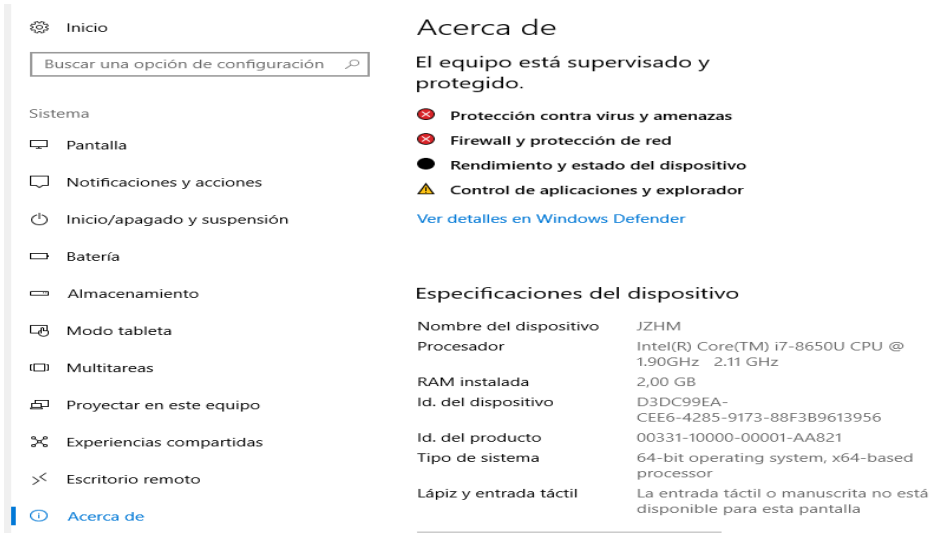
Figura 25 IP Windows



Fuente: Propia

Se procede con la des habilitación del antivirus y firewall según Figura 5

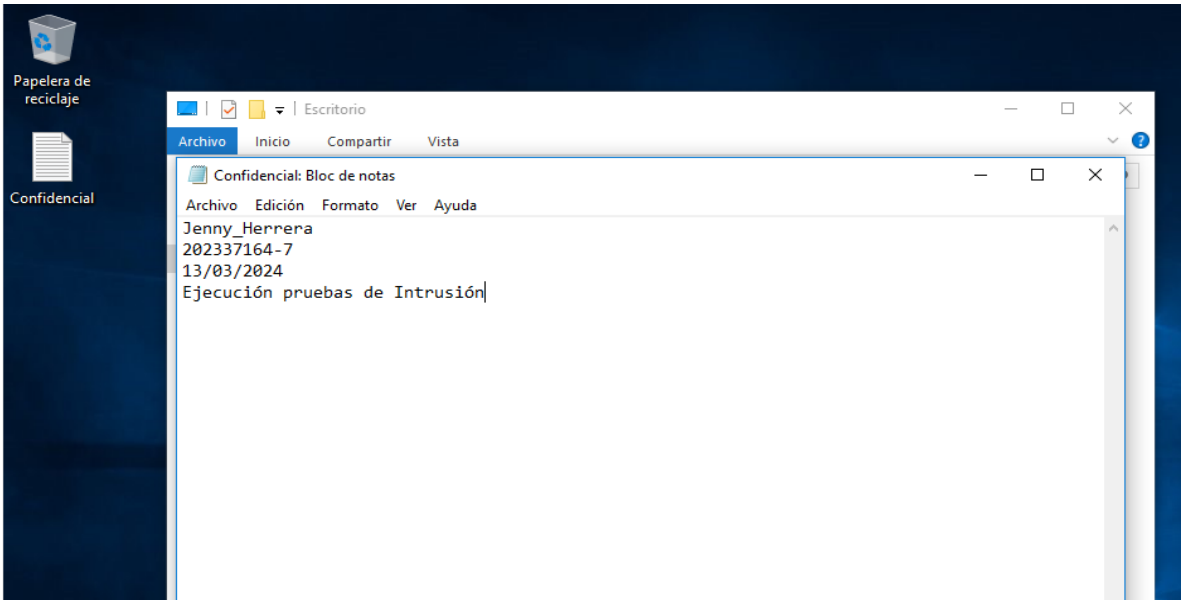
Figura 26 Des habilitación Firewall y Antivirus



Fuente: Propia

Se deja en el escritorio el archivo. Txt el cual llame Confidencia.txt

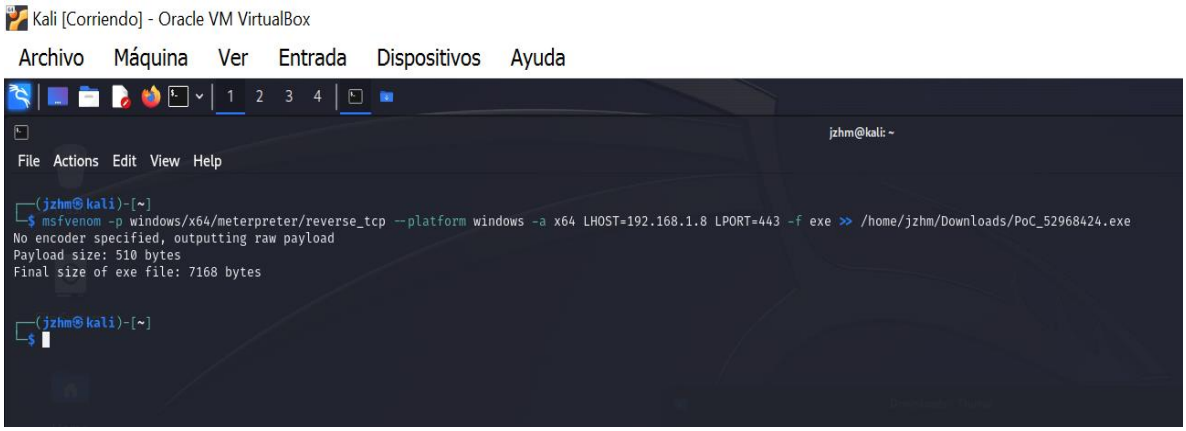
Figura 27. Creación archivo .txt



Fuente: Propia

Se procede con la creación del Payload

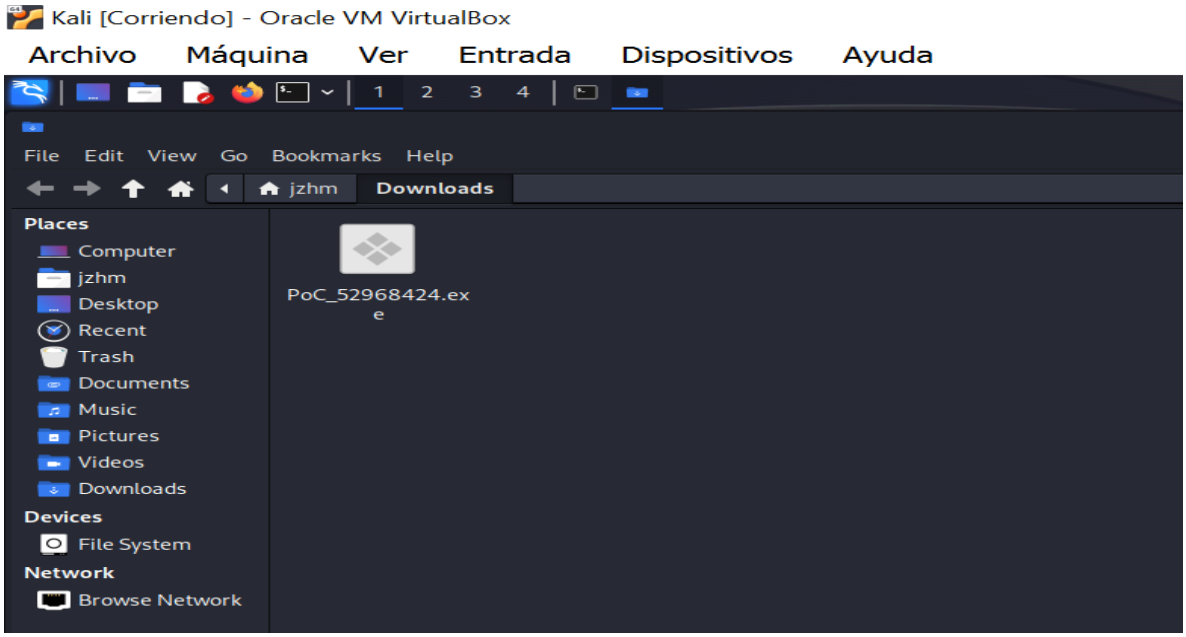
Figura 28. Creación Payload



Fuente: Propia

Se valida que en la ruta elegida este nuestro archivo PoC

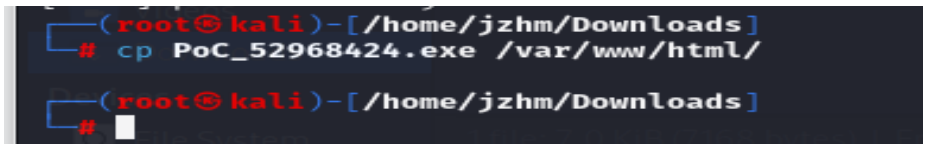
Figura 29. validación archivo POC en Kali



Fuente: Propia

Se enviará archivo por medio de apache2, para esto se instalará el apache y se subirá el servicio, posteriormente se copiará en la ruta /var/www/html/

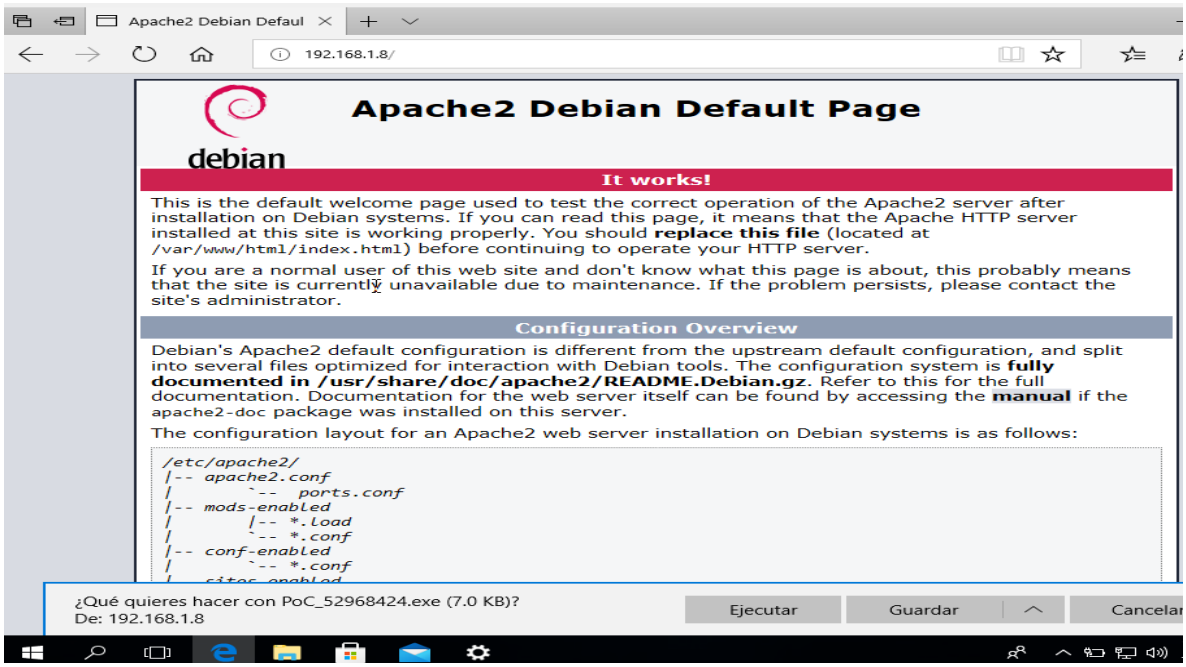
Figura 30.Copia de archivo PoC



Fuente: Propia

Se ejecuta la ip de Kali en el navegador de Windows, en donde descarga el archivo POC

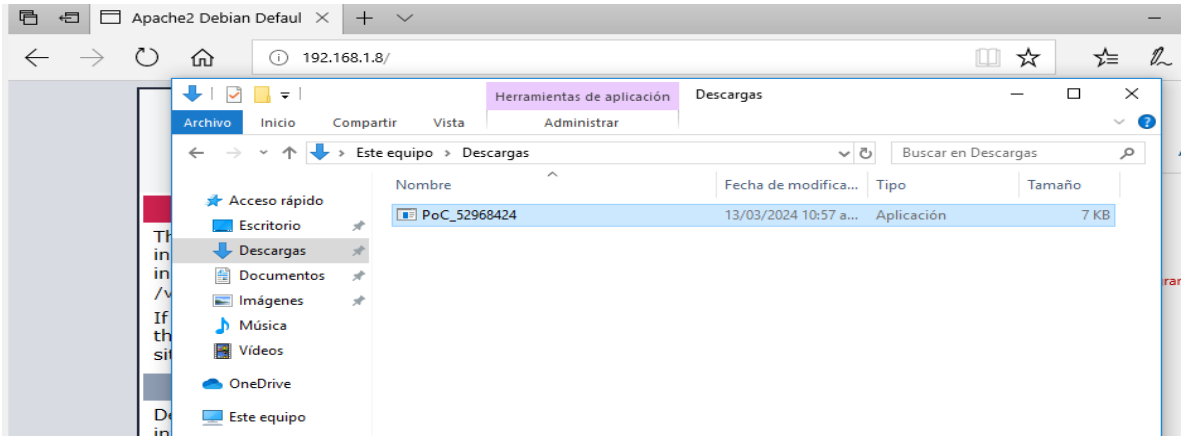
Figura 31. Descarga archivo PoC en windows



Fuente: Propia

Se deja en descargas

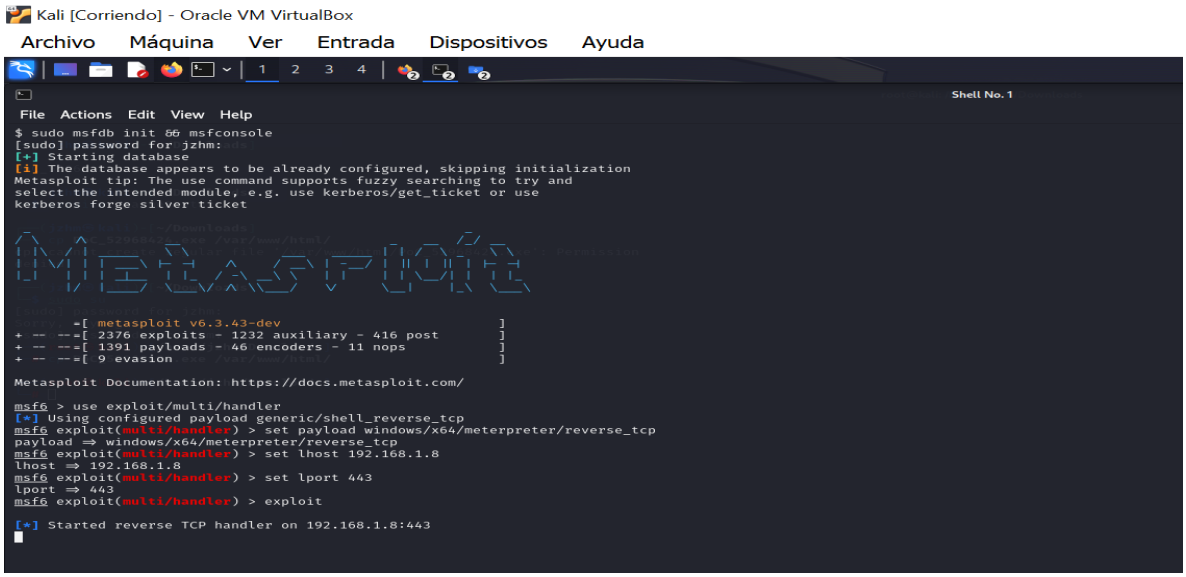
Figura 32. Validación archivo PoC en Windows



Fuente: Propia

Ahora se sube el metasploit y se ejecuta el exploit quedando a la escucha

Figura 33. Metasploit



Fuente: Propia

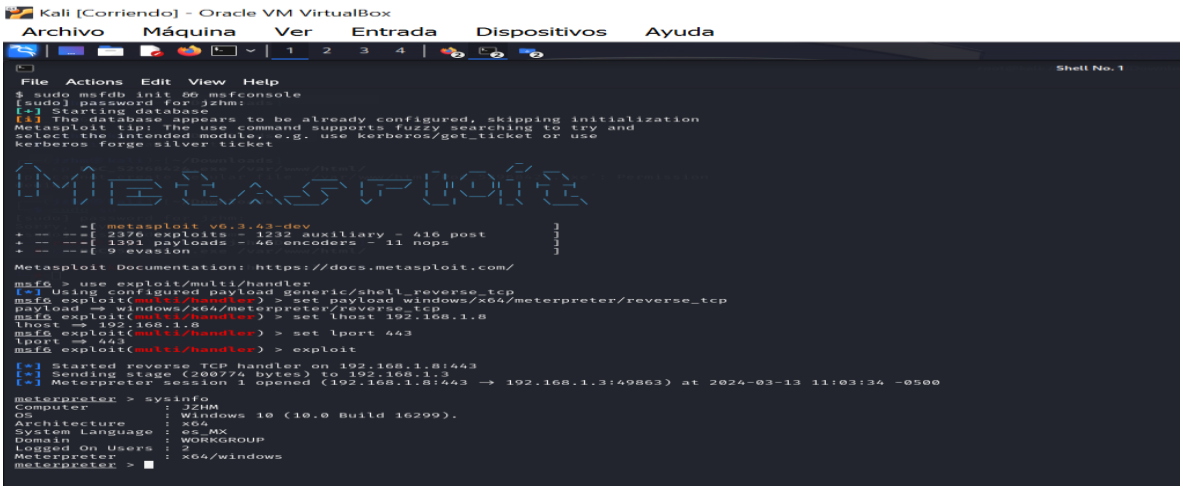
Cuando se ejecuta el archivo en la máquina de Windows, se obtiene acceso

Figura 34. Acceso a la maquina objetivo

Fuente: Propia

El meterpreter se abre y con sysinfo se valida la información de la maquina Windows

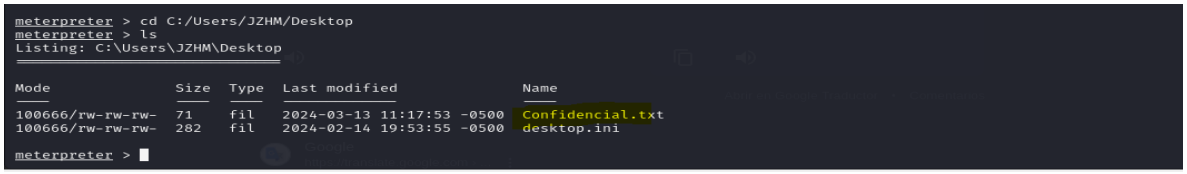
Figura 35. Se obtiene la información de Windows



Fuente: Propia

Se valida la ubicación del archivo y nos cambiamos de directorio ya que está en descargas, pero nuestro documento está en el escritorio

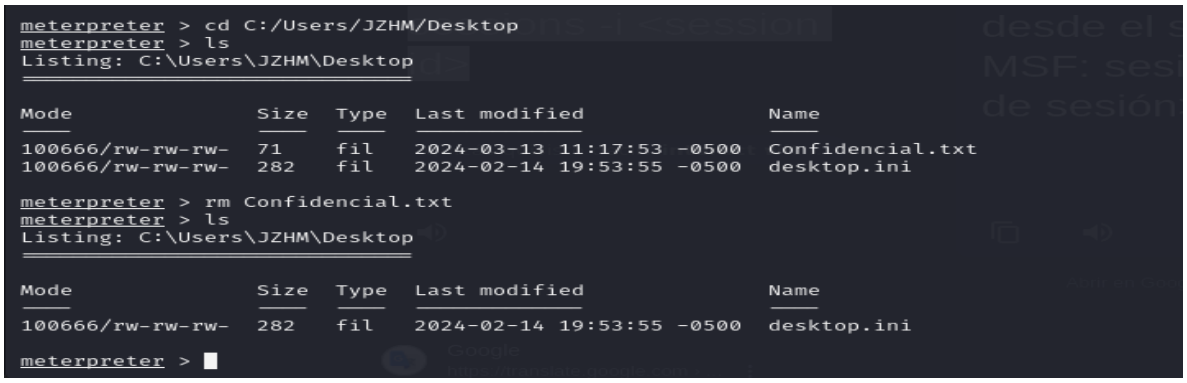
Figura 36. Validación archivo en Windows



Fuente: Propia

Con el comando rm se elimina nuestro archivo Confidencial.txt

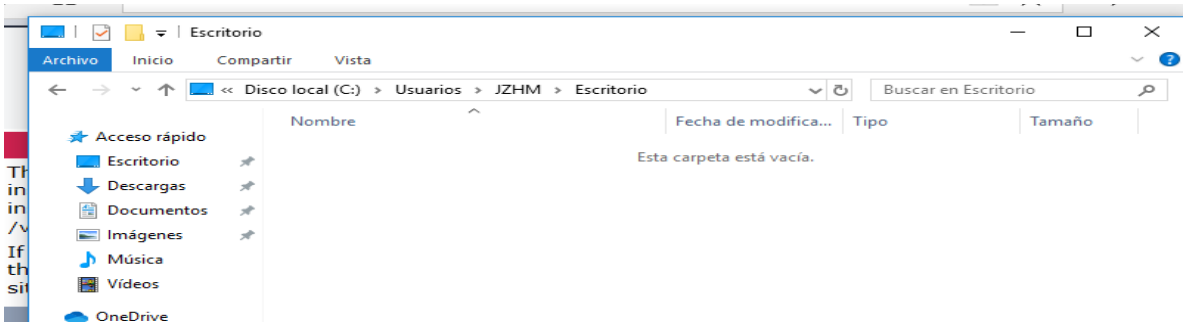
Figura 37. Eliminación archivo Confidencial.txt



Fuente: Propia

Se valida en la máquina de Windows que efectivamente ya no exista el archivo

Figura 38. Confirmación eliminación



Fuente: Propia

17 PASOS PARA LA IDENTIFICACIÓN DE UN ATAQUE

El grupo Blue Team debe estar pendiente ante cualquier actividad sospechosa, como, por ejemplo:

- Incremento de la actividad de archivos inusual.

- Trafico de red sospechoso.

Según el marco de seguridad NIST[19], en su etapa de Detectar, se debe tener en cuenta:

- Los procesos de Detección, se deben probar y actualizar

- Validar y monitorear constantemente los logs. Los registros de eventos contienen iniciación de canales de comunicación, cambios en sistemas o cuentas, por lo tanto, es de gran utilidad para buscar patrones o anomalías.

- Conocer los comportamientos de la empresa y el flujo de datos.

- Cuando se presenta un evento de ciberseguridad, se debe trabajar de manera inmediata para comprender la magnitud del evento.

[19] NIST TECHNICAL SERIES PUBLICATIONS. Primeros pasos de NIST Marco de ciberseguridad: guía de inicio rápido. NIST Technical Series Publications [Sitio web]. (16, marzo, 2022). [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf>.

Dado que la empresa HackerHouse se vio expuesta a un ataque, es importante que el equipo Blue Team, realice la validación y realice los siguientes pasos[20]:

1. Identificar y dejar registrado el incidente: se debe obtener toda la información que esté disponible sobre el incidente y así validar si fue una amenaza real para los sistemas.

2. Evaluar cual fue el alcance del incidente: se debe determinar los datos y sistemas que fueron vulnerados y el grado de afectación.

3. Minimizar el daño: se debe limitar la exposición de los datos o sistemas, tratando de desactivar cuentas, servicios, aplicaciones, bloquear puertos, etc.

4. Restauración de los sistemas y la información: recuperación de archivos perdidos, reconfiguración…

5. Notificar a las autoridades.

6. Seguimiento a los incidentes: es importante realizar monitoreo para que el incidente no se vuelva a presentar.

[20] AUDITECH. ¿Por qué es importante tener un equipo de respuesta a incidentes de ciberseguridad? | Auditech. Auditech [Sitio web]. (10, noviembre, 2023). [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://auditech.es/blog/por-que-es-importante-tener-un-equipo-de-respuesta-a-incidentes-de-ciberseguridad/>.

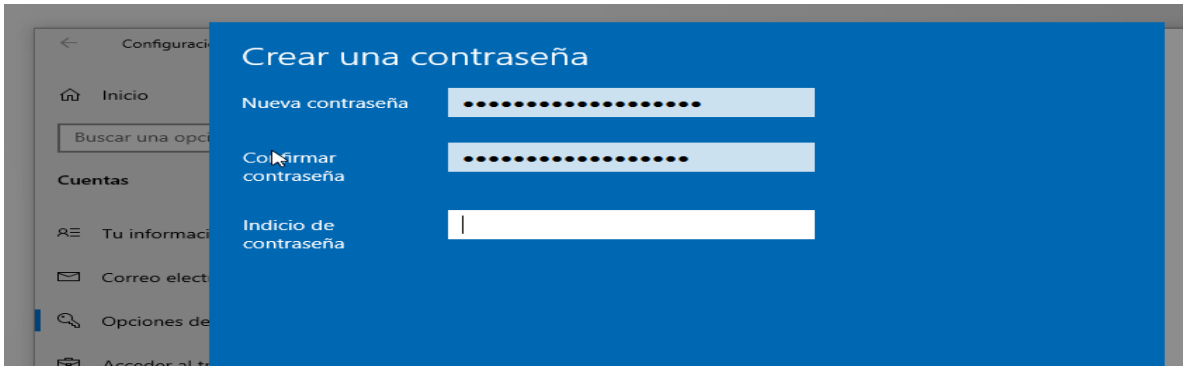
18 PASOS PARA SUBSANAR EL ATAQUE

Teniendo en cuenta los controles del CIS y en cuanto a benchmarks, podemos encontrar, la categoría de sistemas operativos, que son de gran ayuda para la configuración de seguridad, para nuestro caso Windows.

1. Políticas de cuenta: dentro de este control se encuentra las políticas de contraseña, por lo que se debe tener configurado:

La vigencia debe ser 365 días o menos
Longitud mínima 14 o más caracteres
La complejidad debe cumplirse y estar habilitada

Figura 39. Contraseñas

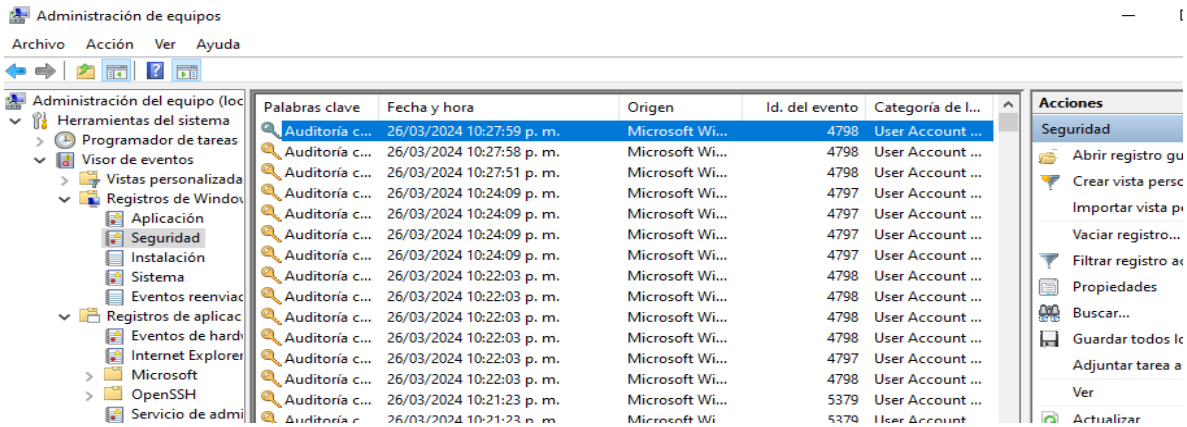


Fuente: Propia

2. Políticas Locales: se debe realizar la configuración de usuarios administradores y locales.

3. Registro de eventos: Se debe validar los logs de eventos y así validar posibles irregularidades.

Figura 40. Registro de eventos



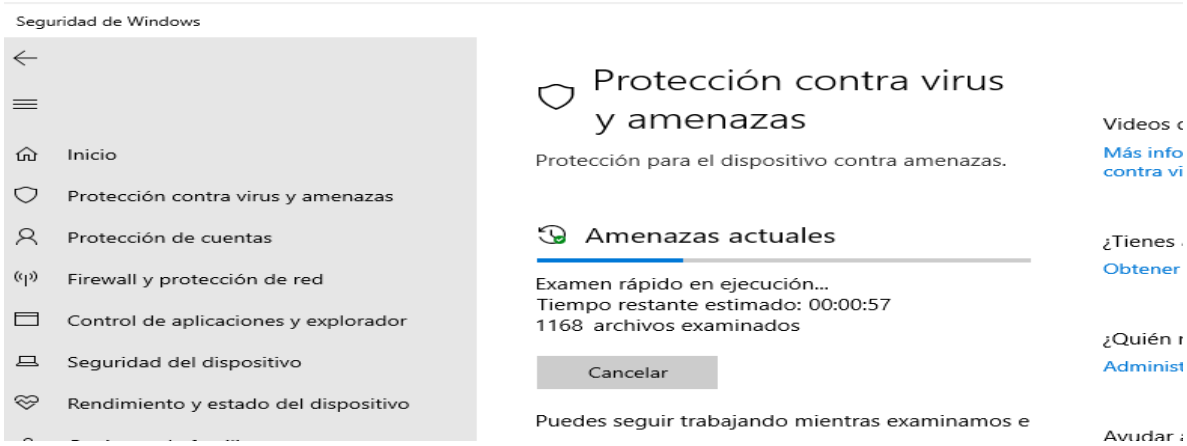
Fuente: Propia

4. Validar que el firewall y antivirus este activo, se activa firewall y antivirus y se procede a realizar un examen

Figura 41. Activación Firewall y antivirus

Fuente: Propia

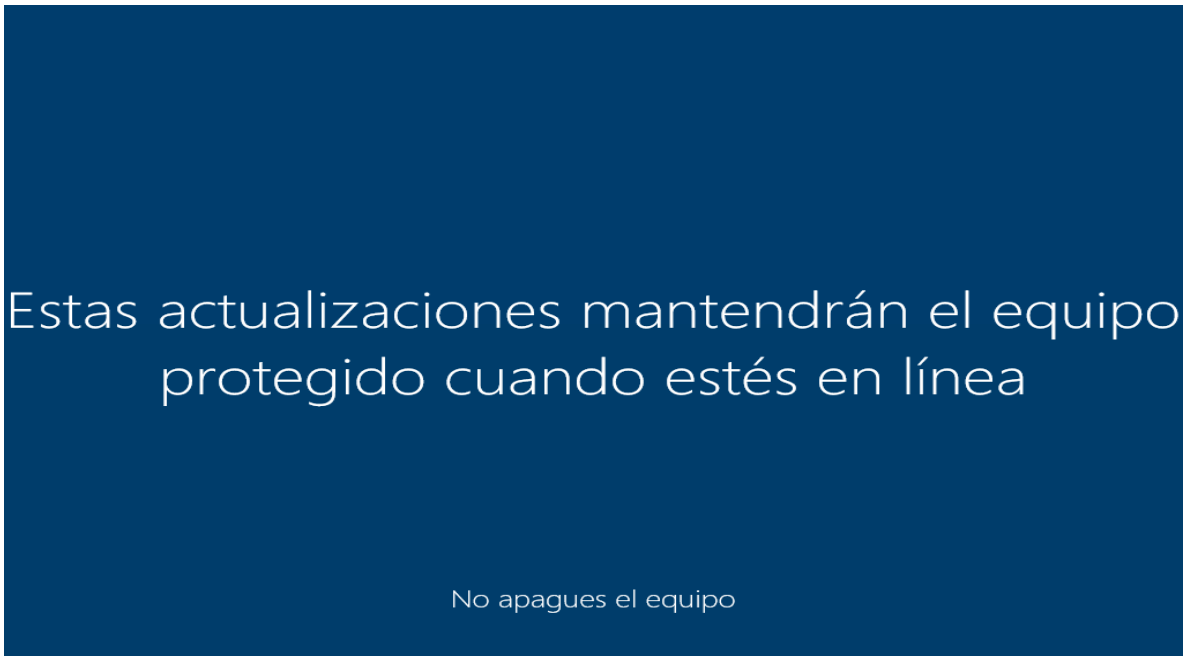
Figura 42. Escaneo con el antivirus



Fuente: Propia

5. Actualización del sistema operativo

Figura 43. Actualización SO



Fuente: Propia

Tabla 4. Diferencias entre los grupos

READ TEAM	BLUE TEAM	PURPLE TEAM	EQUIPO RESPUESTA A INCIDENTES
Seguridad Ofensiva	Seguridad defensiva	Asegura y maximiza la efectividad de los equipos rojo y azul	Son los encargados de recibir los informes, analizarlos y responder a las amenazas.
Emulan a los atacantes	Evalúa las diferentes amenazas	Gestiona seguridad de los activos de la organización	Responde de manera oportuna y urgente contra los ataques.
Emulan escenarios de ataque	Vigilancia constante	Encargados de realizar pruebas	Detienen el impacto del ataque.
Despliegan una serie de pasos para obtener acceso a una red.	Reúne los datos necesarios para saber que hay que proteger,	Busca la integración de tácticas, técnicas y procedimientos ofensivos y técnicas defensivas	Realizan acciones forenses.

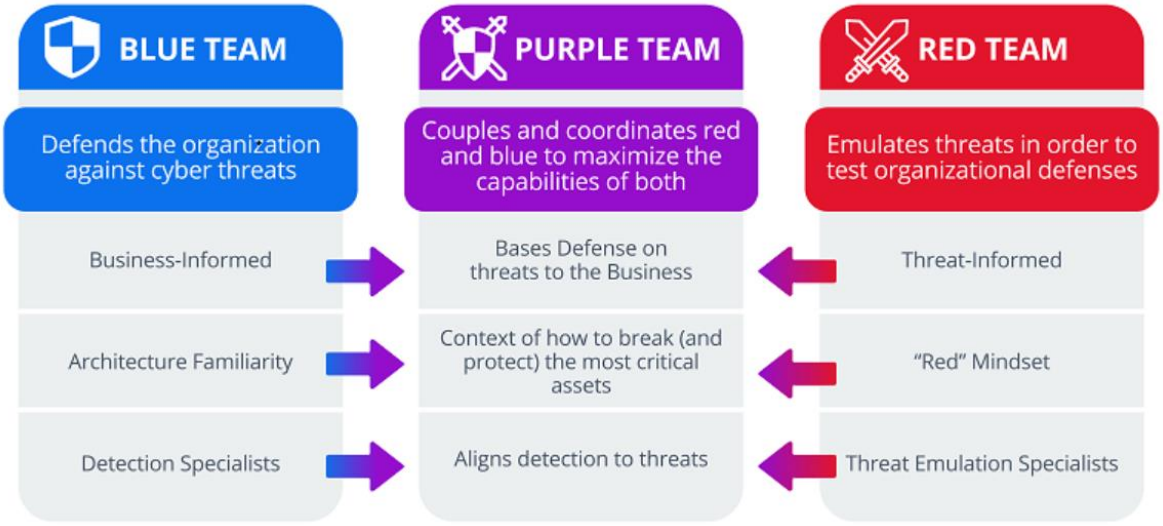
	realizando una evaluación de los riesgos.		
Utilizan rastreadores de paquetes y analizadores de protocolos, con la finalidad de obtener la mayor información posible.	El equipo azul está en la capacidad de reconocer la red y si esta podría estar expuesta a un ataque DDos.	Ayuda que el equipo azul conozca los activos críticos o las brechas de seguridad	Investigan posibles amenazas.
Ejercicios de los equipos rojos: - Pruebas de penetración. - Ingeniería social. - Interceptación de comunicaciones. - Phishing	Ejercicios de los equipos azules: - Auditorias de DNS - Análisis de huella digital. - Validar que los controles de cortafuego estén configurados correctamente.	Ejercicios del equipo morado: - Definir las responsabilidades y roles. - Mediante el CTI se puede analizar y recopilar información necesaria. - Organizar y analizar. - Tener un plan de desarrollo.	Ejercicios del equipo de respuesta a incidentes: - Tomar medidas para prevenir los incidentes. - Actualizar, probar y gestionar el plan de respuestas a incidentes. - Ubicar en cuarentena y aislar sistemas.

	- Desplegar control de seguridad de detección y prevención. - Aseguramiento de los sistemas.	- Ejecución del plan.	- Actividades de seguimiento, documentación, análisis e identificación de los incidentes.

Fuente: Propia

En la figura 44, se puede observar la función más importante y la característica de los tres grupos

Figura 44. Características y funciones de los tres grupos



Fuente: INCIBE. El equipo púrpura aumenta la efectividad del equipo rojo y el equipo azul en SCI. INCIBE [Sitio web]. (23, julio, 2023). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.incibe.es/en/incibe-cert/blog/purple-team-increases-effectiveness-red-team-and-blue-team-sci>.

20 CIS “CENTER FOR INTERNET SECURITY”

Los controles de seguridad críticos CIS[21] son un conjunto de recomendaciones para la ciberdefensa que brindan formas determinadas y viables de frustrar los ataques. Los controles CIS son una lista de acciones defensivas que ayudan a tener un punto de partida de lo que se debe hacer y lo que primero se debe hacer, para mejorar la seguridad.

Beneficios:

- Ayuda a las organizaciones a tener el punto de partida en la defensa.
- Dirigir los recursos en acciones inmediatas.
- Centrar la atención la atención y recursos, según los riesgos que son exclusivos del negocio.

Los controles CIS se pueden utilizar con los marcos regulatorios como, por ejemplo, NIST, ISO27000 y regulaciones como PCI DSS, HIPAA, NERC CIP y FISMA

Actualmente cuenta con 18 controles, que se relacionan a continuación[22]:

Control CIS 1: Inventario y Control de Activos Empresariales

Control CIS 2: Inventario y Control de Activos de Software

Control CIS 3: Protección de datos

Control CIS 4: Configuración segura de software y activos empresariales

[21] CIS. CIS critical security controls FAQ. CIS [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cisecurity.org/controls/cis-controls-faq>.
[22] --------. The 18 CIS controls. CIS [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cisecurity.org/controls/cis-controls-list>.

Control CIS 5: Gestión de cuentas

Control CIS 6: Gestión del control de acceso

Control CIS 7: Gestión continua de vulnerabilidades

Control CIS 8: Gestión de registros de auditoría

Control CIS 9: Protecciones de correo electrónico y navegador web

Control CIS 10: Defensas contra malware

Control CIS 11: Recuperación de datos

Control CIS 12: Gestión de infraestructura de red

Control CIS 13: Monitoreo y defensa de la red

Control CIS 14: Concientización sobre seguridad y capacitación en habilidades

Control CIS 15: Gestión de proveedores de servicios

Control CIS 16: Seguridad del software de aplicaciones

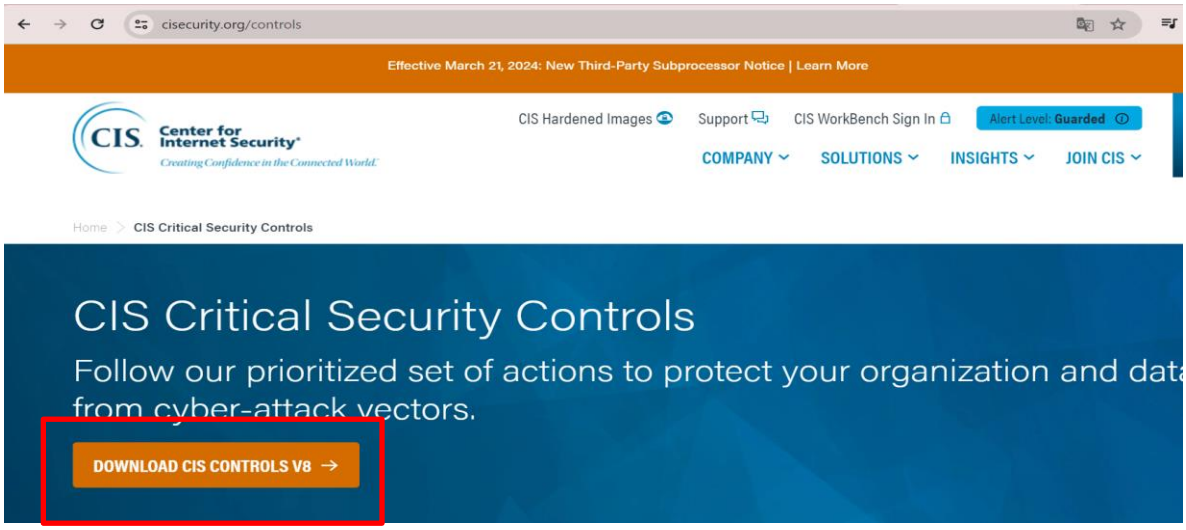
Control CIS 17: Gestión de respuesta a incidentes

Control CIS 18: Pruebas de penetración

Dado que el equipo blue team, se encarga de la seguridad defensiva y de evaluar las diferentes amenazas, los controles CIS, son de gran ayuda y es una herramienta que proporciona una serie de pasos para validar que tan asegurado esta nuestro sistema, Los CIS también tienen unos controles específicos que nos ayuda dependiendo la necesidad que se tenga, ahora veremos como podemos descargar los controles, ya que son gratuitos.

En el paso 1, ubicamos la opción para descargar

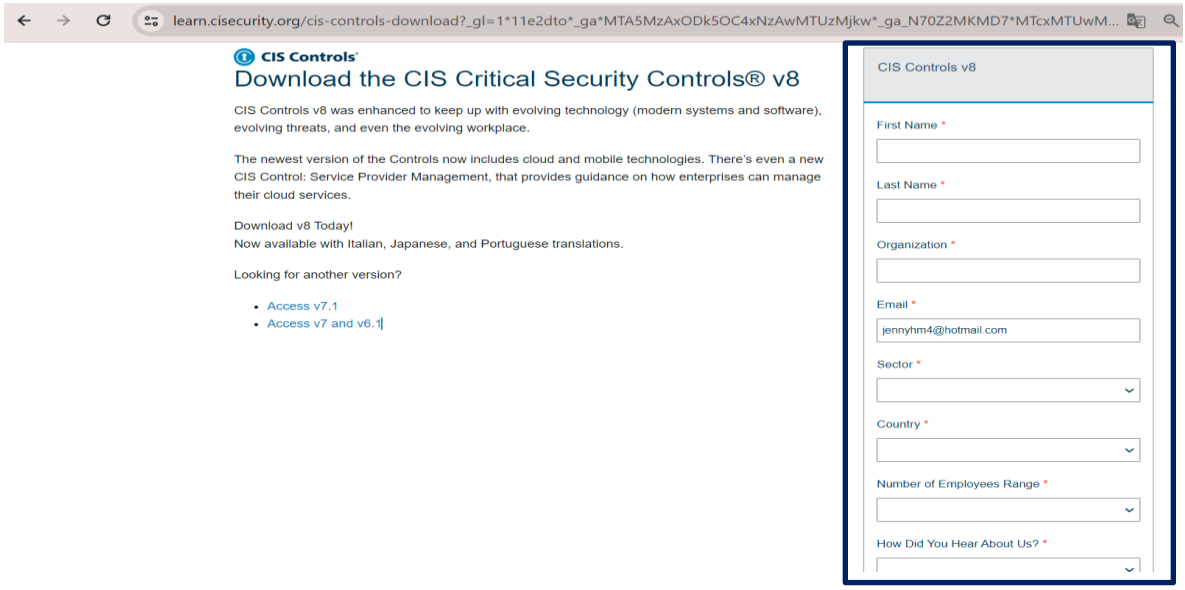
Figura 45. Paso 1



Fuente: Propia

En el paso 2, nos solicita información básica, en donde la diligenciamos para obtener el Pdf

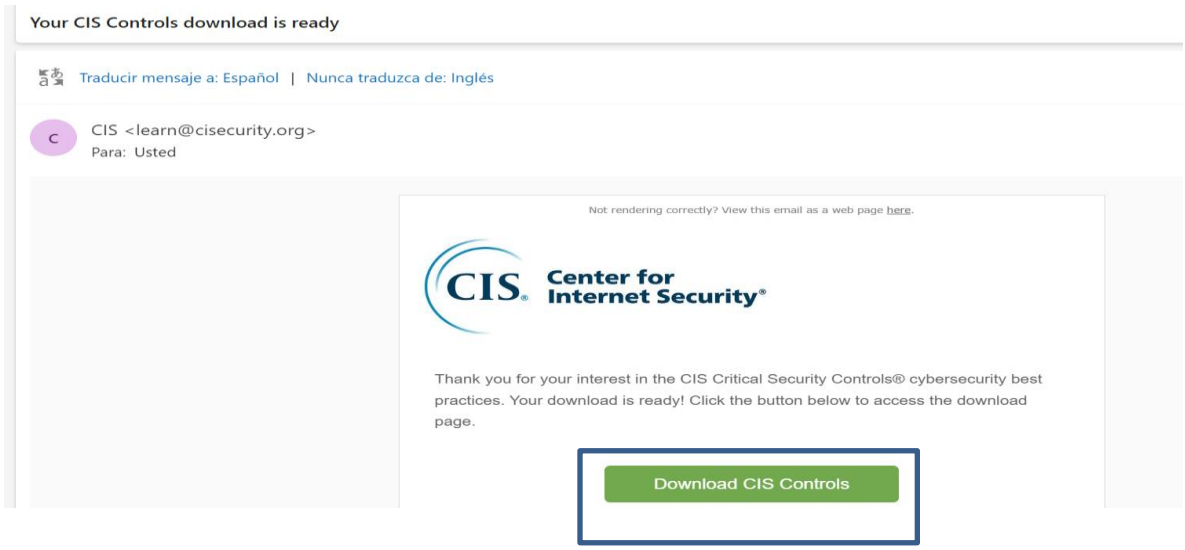
Figura 46. Paso 2



Fuente: Propia

En el paso 3 nos llega un correo que nos da un enlace

Figura 47. Paso 3



Fuente: Propia

Cuando damos click en el link, nos lleva a la página y podremos descargar el PDF con los controles, actualmente está la V8 pero si uno quiere también puede descargar la V7.1

Figura 48. Paso 4

Fuente: Propia

21 DIFERENCIAS SIEM Y XDR

Tabla 5. Diferencias entre SIEM y XDR

	SIEM	XDR
OBJETIVO	Gestión centralizada y análisis de registros, correlaciona datos de varias soluciones, para realizar un análisis posterior	Centra el uso de los datos que obtiene para mejorar la respuesta, ya que identifica, investiga y toma las medidas necesarias para resolver los incidentes de manera ágil
COMPLEJIDAD DE GESTIÓN	Son de naturaleza abierta, debido al gran volumen de información,	Su arquitectura es más sencilla y tiene la gran ventaja de reducir alertas

	producen gran cantidad de alertas individuales, lo que lo hace un poco difícil de clasificar.	importantes, ayudando a priorizar las acciones a tomar.
ALMACENAMIENTO DE DATOS	Sirven como almacén central y a largo plazo	Accede a datos de otras fuentes, pero los almacena temporalmente.
CAPACIDAD DE RESPUESTA	Tienen alguna capacidad de respuesta, proporciona datos a los MSP y genera alertas que son útiles para la identificación de amenazas.	Tiene la posibilidad de apoyar y coordinar la respuesta, en la misma solución.

Fuente: ARNAL, Carlos. ¿Cuál es la diferencia entre XDR y SIEM? | WatchGuard Technologies. WatchGuard | Network, Wi-Fi, Identity, and Endpoint Security Solutions [Sitio web]. (8, mayo, 2023). [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem>.

22 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

22.1 SNORT

Este es un sistema de prevención de intrusiones IPS, utiliza una serie de reglas que ayudan a la identificación de actividades sospechosas sobre la red, logrando encontrar paquetes que permitan el alertamiento para los usuarios. Esta herramienta también puede ser útil para la depuración de trafico de red[23].

Figura 49. Snort

Fuente: GITHUB. GitHub - WhiteHatCyberus/SNORT-GUI: SNORT GUI: Your very own trusted blueteam forensic companion for SNORT IDS. OPTIMIZED, SECURE AND ABSOLUTELY FREE! [imagen]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://github.com/WhiteHatCyberus/SNORT-GUI>.

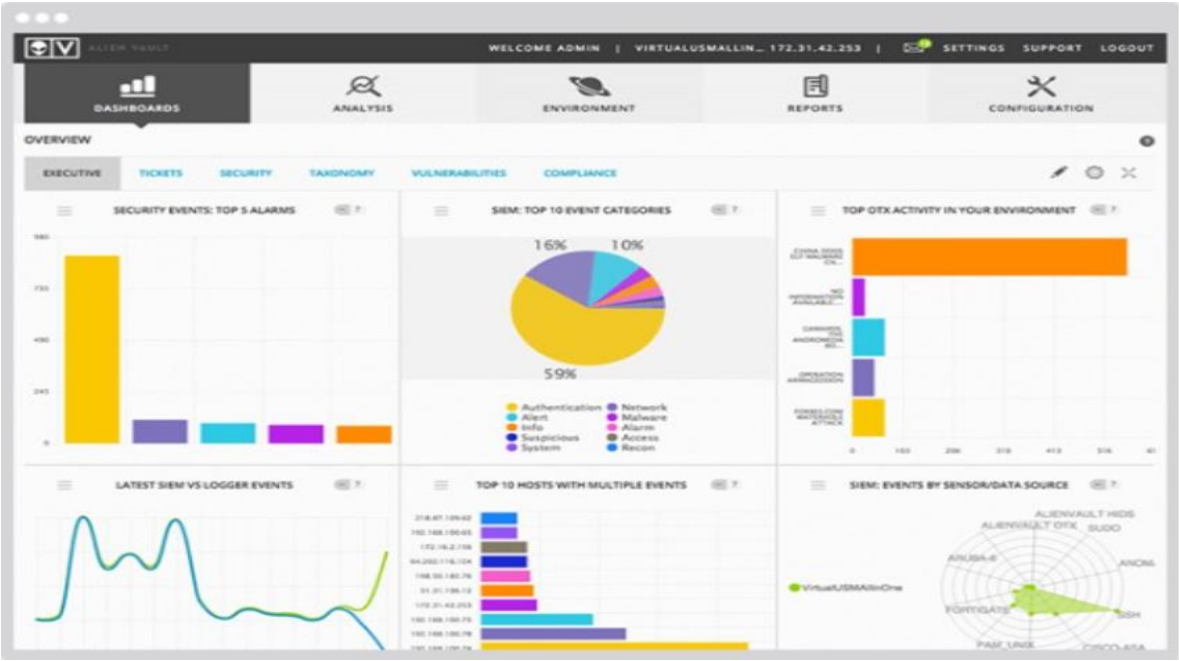
[23] SNORT. What is snort? https://www.snort.org/ [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.snort.org/>.

22.2 OSSIM

Siendo la abreviatura de (Sistema de gestión de la información de seguridad Open Source), Es una herramienta de gestión de eventos y seguridad (SIEM), incluye la normalización, recopilación y la correlación de eventos, esta plataforma tiene muchas capacidades como:

Descubrimiento de activos
Evaluación de vulnerabilidad
Detección de intrusiones
Monitoreo del comportamiento
Correlación de eventos SIEM

Figura 50. Panel OSSIM



Fuente: CARDONA, Herm. AlienVault OSSIM Guide [imagen]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.winmill.com/securing-your-work-from-home-network/>.

22.3 ARKIME

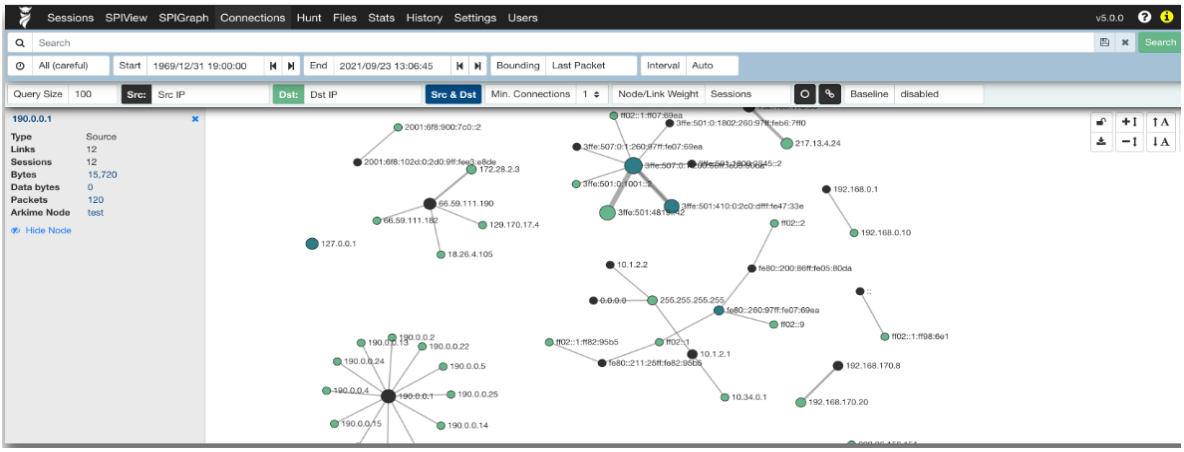
Es una herramienta que tiene visibilidad total de la red, por lo que facilita la identificación y solución de problemas de la red y seguridad[24]. Algunas de las características son:

- Se obtiene acceso a los datos, por lo que los grupos de seguridad tienen visibilidad de la red y pueden responder de una manera más ágil e investigar de manera global el incidente.

- Se puede implementar en varios sistemas en clúster.

- Los grupos de seguridad pueden responder, investigar, reconstruir y confirmar las amenazas en la red y responder de una manera adecuada.

Figura 51. Página de conexiones



Fuente: ARKIME. Arkime. Arkime [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://arkime.com/>.

[24] ARKIME. Arkime. Arkime [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://arkime.com/>.

23 APORTE EN LA CIBERSEGURIDAD DE LOS GRUPOS RED TEAM, BLUE TEAM Y PURPLE TEAM

Son varios los beneficios que encontramos al tener en la organización funcionando los tres grupos, estos dan más seguridad a la infraestructura e información, estos son algunos puntos claves[25]:

- Cuando actúa el grupo Red Team y el grupo Blue Team se puede lograr una identificación de vulnerabilidades, ya que el grupo red se encarga de descubrir la debilidad, mientras el grupo blue realiza ejercicios de mitigación.

- La colaboración de los dos grupos permite una respuesta más rápida y efectiva frente a las amenazas que se puedan presentar.

- El grupo Red Team puede realizar evaluaciones continuas, lo que permite robustecer la seguridad.

- Dado que el grupo Red está en constante estudio de las nuevas técnicas de ataque, el grupo Blue se beneficia y les permite estar mejor preparados.

- Se obtiene un ahorro en los costos, ya que los grupos al realizar de manera proactiva la identificación de vulnerabilidades, logran contener aquellas vulnerabilidades que pueden llegar a costar bastante dinero si se efectúa el ataque.

- La sinergia de los grupos hace que las organizaciones estén preparadas y aseguren sus activos críticos.

- La implementación de los grupos mejora la cultura en la seguridad, ya que se vuelve una prioridad para todos los empleados.

[25] SÁNCHEZ RODRÍGUEZ, Alfonso. Red team, blue team y purple team - dolbuck ciberseguridad. Dolbuck - Empresa de Ciberseguridad en Sevilla [Sitio web]. (17, agosto, 2023). [Consultado el 3, abril, 2024]. Disponible en Internet: <https://dolbuck.net/ciberseguridad/red-team-blue-team-purple-team/#:~:text=Beneficios%20del%20Red%20Team,%20Blue%20Team%20y%20Purple%20Team,-La%20colaboración%20es&text=Mejora%20de%20la%20detección%20y,efectiva%20ante%20incidentes%20de%20seguridad.>.

24 RECOMENDACIONES DE SEGURIDAD

Las organizaciones deben enfocarse en invertir en seguridad, ya que si se llegara a presentar un ataque que conlleve a la operación critica, puede salir mas costoso reparar el daño, que la misma inversión que re realice en seguridad, aquí se mencionan algunas recomendaciones[26]:

- Es importante invertir en seguridad, teniendo claros las amenazas a las que puede estar expuesta la organización.
- Tener planes de contingencia para mantener a salvo la información.
- Tener medidas preventivas.
- Proteger la información y los activos mas importantes de la organización.
- Capacitaciones a los empleados, ya que son los principales focos de ingeniería social.
- Se debe complementar las medidas preventivas, teniendo un monitoreo constante del flujo de la información.

También es importante realizar unas validaciones previas antes de la elaboración de políticas e implementar las medidas de seguridad al interior de la organización[27]:

[26] KPMG. Ciberseguridad siete medidas básicas para proteger la empresa. KPMG Global [Sitio web]. [Consultado el 3, abril, 2024]. Disponible en Internet: <https://assets.kpmg.com/content/dam/kpmg/mx/pdf/2018/04/ciberseguridad-servicios.pdf>.

[27] MINTIC. Guía para la implementación de seguridad de la información en una MIPYME. https://gobiernodigital.mintic.gov.co/ [Sitio web]. [Consultado el 3, abril, 2024]. Disponible en Internet: <https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf>.

Identificación de los activos de la organización

Realizar un inventario de los activos, donde se debe tener en cuenta, el tipo de activo, la descripción, propietario, personas que lo utiliza, si existe custodio del activo y la ubicación.

Establecer las posibles vulnerabilidades a las que se ve expuesta la organización

Dado que existen varias vulnerabilidades, se deben establecer las relacionadas con temas naturales, físicos, Software y Hardware, comunicaciones, humanas y las que se puedan evidenciar en el entorno de la organización.

Clasificar las amenazas

Es importante tener presente que cuando ya se presenta la amenaza, es porque esta se presentó ya que existe una vulnerabilidad, las amenazas pueden generar interrupción, modificación, generación o intercepción del sistema.

Evaluar los riesgos a los que está expuesta la organización

Para ello se deben tener en cuenta los dos puntos anteriores, y así poder realizar la construcción de una metodología para la valoración de riesgo basado en un adecuado SGSI.

25 LINK DEL VIDEO

https://drive.google.com/file/d/1H4hI8rkGUuI9MAame1gWJL1DPiJ1xJGV/view?usp=drive_link

CONCLUSIONES

Es importante conocer y tener claras las leyes que dan la protección a la información y que regula el manejo de los datos de los usuarios, es por eso que en este informe técnico, se analizó la ley 1273 de 2009, que sanciona aquellos delitos que van en contra de los pilares de la seguridad de la información, en donde se tipifican 9 delitos, entre los cuales se encuentran: Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, e Interceptación de datos informáticos y La ley 1581 DE 2012, que tiene como objeto el derecho constitucional que tiene toda persona a conocer, actualizar y modificar la información que se encuentra relacionada en cualquier base de datos.

Se pudo establecer la importancia de tener dentro de las organizaciones, los equipos red team y blue team, ya que estos realizan las acciones tanto de prevención como la detección de vulnerabilidades y así se logra identificar aquellos puntos en los que la organización esta débil, para fortalecer su seguridad y evitar que los riesgos se materialicen.

También es importante tener el personal capacitado y utilizar las herramientas adecuadas para la detección de vulnerabilidades y a su vez aquellas herramientas que nos ayudaran a la protección, teniendo una buena comunicación entre equipos y de allí nace la importancia del grupo purple team, ya que ellos garantizan que se comparta la información entre el equipo blue team y red team.

Por ultimo y lo más importante de las organizaciones, es su personal, ya que es el principal foco de los cibercriminales, por ello es importante siempre realizar capacitaciones sobre ciberseguridad, y así convertir a los empleados en la primera línea de defensa.

BIBLIOGRAFÍA

ARKIME. Arkime. Arkime [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://arkime.com/>.

ARNAL, Carlos. ¿Cuál es la diferencia entre XDR y SIEM? | WatchGuard Technologies. WatchGuard | Network, Wi-Fi, Identity, and Endpoint Security

AUDITECH. ¿Por qué es importante tener un equipo de respuesta a incidentes de ciberseguridad? | Auditech. Auditech [Sitio web]. (10, noviembre, 2023). [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://auditech.es/blog/por-que-es-importante-tener-un-equipo-de-respuesta-a-incidentes-de-ciberseguridad/>.

CARDONA, Herm. AlienVault OSSIM Guide [imagen]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.winmill.com/securing-your-work-from-home-network/>.

CIBERSEG1922. Footprinting y fingerprinting | ciberseguridad. Ciberseguridad [Sitio web]. (9, diciembre, 2019). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://ciberseguridad.com/amenzas/footprinting-fingerprinting/>.

CIS. CIS critical security controls FAQ. CIS [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cisecurity.org/controls/cis-controls-faq>.

CYBERZAINTZA. Equipo de respuesta ante incidentes | Cyberzaintza. Inicio | Cyberzaintza [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.ciberseguridad.eus/ciberglosario/equipo-de-respuesta-ante-incidentes>.

ESTEFANÍA DOMÍNGUEZ DE LA IGLESIA. ¿Qué es el pentesting? Campus Internacional de Ciberseguridad [Sitio web]. (26, febrero, 2020). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting>.

FISCALÍA GENERAL DE LA NACIÓN. Cartilla metodológica de atención de delitos informáticos. Fiscalia General de la Nación [Sitio web]. (21, septiembre, 2023). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf>.

FISCALÍA GENERAL DE LA NACIÓN. Cartilla metodológica de atención de delitos informáticos. Fiscalia General de la Nación [Sitio web]. (21, septiembre, 2023). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf>.

GITHUB. GitHub - s0md3v/photon: incredibly fast crawler designed for OSINT. GitHub [Sitio web]. [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://github.com/s0md3v/Photon>.

GITHUB. GitHub - WhiteHatCyberus/SNORT-GUI: SNORT GUI: Your very own trusted blueteam forensic companion for SNORT IDS. OPTIMIZED, SECURE AND ABSOLUTELY FREE! [imagen]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://github.com/WhiteHatCyberus/SNORT-GUI>.

GONZÁLEZ, Sol. Maltego, la herramienta que te muestra qué tan expuesto estás en Internet. Award-winning news, views, and insight from the ESET security community [Sitio web]. (11, mayo, 2023). [Consultado el 18, febrero, 2024]. Disponible en Internet: <https://www.welivesecurity.com/la-es/2023/05/11/maltego-herramienta-muestra-tan-expuesto-estas-internet/>.

H1RD. Introducción a metasploit. H1RD.COM [Sitio web]. (2, agosto, 2017). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://www.h1rd.com/hacking/Introduccion-a-metasploit>.

INCIBE. El equipo púrpura aumenta la efectividad del equipo rojo y el equipo azul en SCI. INCIBE [Sitio web]. (23, julio, 2023). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.incibe.es/en/incibe-cert/blog/purple-team-increases-effectiveness-red-team-and-blue-team-sci>.

INTELEQUIA. Red team y blue team - funciones y diferencias en ciberseguridad. Intelequia [Sitio web]. (26, enero, 2021). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad>.

KALI LINUX. Recon-ng | kali linux tools. Kali Linux [Sitio web]. (16, febrero, 2024). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://www.kali.org/tools/recon-ng/>.

KASPERSKY. ¿Qué es una huella digital? ¿Cómo podemos protegerla de los hackers? latam.kaspersky.com [Sitio web]. [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://latam.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>.

KEEPCODING. ¿Qué es ExploitDB? | KeepCoding Bootcamps. KeepCoding Bootcamps [Sitio web]. [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-exploitdb/>.

KEEPCODING. Fases de un pentest | KeepCoding Bootcamps. KeepCoding Bootcamps [Sitio web]. (28, julio, 2023). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/>.

NIST TECHNICAL SERIES PUBLICATIONS. Primeros pasos de NIST Marco de ciberseguridad: guía de inicio rápido. NIST Technical Series Publications [Sitio web]. (16, marzo, 2022). [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf>.

RED HAT. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [Sitio web]. (15, noviembre, 2021). [Consultado el 17, febrero, 2024]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve>.

SECRETARÍA GENERAL DEL SENADO. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. SECRETARÍA GENERAL DEL SENADO [Sitio web]. (31, diciembre, 2023). [Consultado el 15, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>.

SECRETARÍA GENERAL DEL SENADO. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. SECRETARÍA GENERAL DEL SENADO [Sitio web]. (31, diciembre, 2023). [Consultado el 15, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>.

SHEA, Sharon y IREI, Alissa. ¿Qué es ¿Qué es la respuesta a incidentes? ¿Planes, equipos y herramientas? - Definición en Computer Weekly. ComputerWeekly.es [Sitio web]. (13, abril, 2023). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.computerweekly.com/es/definicion/Que-es-la-respuesta-a-incidentes-Planes-equipos-y-herramientas>.

SNORT. What is snort? https://www.snort.org/ [Sitio web]. [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.snort.org/>.

Solutions [Sitio web]. (8, mayo, 2023). [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem>.

TARLOGIC SECURITY. Blue Team: fortalecer la defensa de una compañía. Tarlogic Security [Sitio web]. [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://www.tarlogic.com/es/blog/blue-team/>.

UNIR. Red team, blue team y purple team: funciones y diferencias. UNIR [Sitio web]. (7, enero, 2020). [Consultado el 25, marzo, 2024]. Disponible en Internet: <https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/>.