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

MARCELA ALEJANDRA ASTORQUIZA LÓPEZ

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

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

MARCELA ALEJANDRA ASTORQUIZA LÓPEZ

Informe Técnico presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

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
MEDELLÍN
2024

RESUMEN

Este informe técnico se centra en las características y aportes de los equipos Red Team y Blue Team en la evaluación y optimización de la ciberseguridad en las organizaciones.

A través de un enfoque teórico-práctico dividido en cinco fases (Conceptos, Actuación legal, Pruebas de intrusión, Contención de ataques y Socialización de informe) y el uso de herramientas especializadas, se analizan las estrategias y metodologías empleadas por estos equipos para identificar y mitigar vulnerabilidades en los sistemas informáticos de la empresa "HackerHouse"

El documento surge como resultado del seminario "Equipos estratégicos en ciberseguridad: Red team & Blue team", donde se busca fomentar la capacidad de investigación e innovación de los estudiantes en el ámbito de la Ciberseguridad y la Seguridad de la Información.

Palabras clave: Ciberseguridad, Red Team, Blue Team, Seguridad de la información, Herramientas de Ciberseguridad.

ABSTRACT

This technical report focuses on the characteristics and contributions of the Red Team and Blue Team teams on the evaluating and optimizing cybersecurity within organizations.

Through a theoretical-practical approach divided into five phases (Concepts, Legal Action, Intrusion Testing, Attack Containment, and Report Socialization) and the use of specialized tools, strategies and methodologies are used by these teams to identify and mitigate vulnerabilities in the enterprise computer systems of "HackerHouse".

The document emerges as a result of the seminar "Strategic teams in cybersecurity: Red team & Blue team", wich is looking to promote the research and innovation capacity of students in the field of cybersecurity and information security.

Keywords: Cybersecurity, Red Team, Blue Team, Information Security, Cybersecurity Tools.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: Datos y recursos de software/hardware que contienen información crítica para las organizaciones y sus operaciones.

BLUE TEAM: Equipo de trabajo conformado para la defensa reactiva y preventiva frente a las amenazas cibernéticas de manera rápida y eficaz.

CIBERSEGURIDAD: Conjunto de estrategias y recursos utilizados para salvaguardar los activos de información contra ataques digitales

CUMPLIMIENTO CONTRACTUAL: Hace referencia al cumplimiento de contratos u obligaciones establecidas con terceros (empresas/personas)

COPNIA: Consejo profesional nacional de ingeniería en Colombia, entidad encargada de supervisar y controlar la práctica de la ingeniería en el país.

CVSS (Common Vulnerability Score System): Es un marco estandarizado para evaluar y estimar la severidad de las debilidades en los activos de información.

ETHICAL HACKING: Salvaguarda los recursos de información de una organización mediante la simulación de ataques cibernéticos, con el objetivo de detectar y corregir posibles vulnerabilidades que puedan afectar el funcionamiento de los sistemas.

EXPLOIT: Código desarrollado para aprovechar y explotar las vulnerabilidades de los sistemas informáticos a través de la carga de códigos maliciosos.

FIREWALL: Sistema de seguridad perimetral que se utiliza para controlar el tráfico de entrada y salida en la red, limitando las comunicaciones permitidas en los entornos organizacionales.

FUGA DE INFORMACIÓN: Es la perdida no autorizada de información confidencial que debe ser protegida.

GESTIÓN DE RIESGOS: Proceso diseñado para la tipificación, análisis y evaluación para tratar riesgos potenciales que puedan afectar a las empresas, minimizando las perdidas relacionadas a incidentes de seguridad.

HARDENING: Es el proceso de robustecimiento de las capacidades y seguridad de un sistema o red para reducir las superficies de ataques de Ciberseguridad

MALWARE: Programa de software diseñado de forma malintencionada para ejecutar acciones dañinas en un sistema informático

PAYLOAD: Es el núcleo funcional de paquetes de instrucciones que se desencadenan al ejecutar un exploit en una máquina que van desde infectar con software malicioso, escalamiento de privilegios, robo de información, entre otros.

PURPLE TEAM: Equipo de trabajo hibrido que combina las capacidades de los Red Team y Blue Team para la ejecución de pruebas de seguridad de forma colaborativa y transparente con todos los responsables funcionales y técnicos.

RED TEAM: Equipo de trabajo conformado para la simulación de ataques cibernéticos en organizaciones.

RIESGO CIBERNÉTICO: La posibilidad de que un evento desfavorable afecte la seguridad de los sistemas informáticos, redes o datos de una entidad.

VULNERABILIDAD INFORMÁTICA: Son las debilidades del sistema informático, red o datos que puede ser aprovechado por un atacante para obtener acceso o causa daños a los servicios e información.

INTRODUCCIÓN

Durante los últimos cinco años, la tendencia de los ataques cibernéticos en Colombia ha ido en aumento. En 2022 se registró una tasa de crecimiento del 26% más alta que la del año 2021[1]. Las consecuencias de estos eventos suelen ser devastadoras para las empresas, ya que pueden causar la pérdida no solo de información, sino también daños reputacionales y financieros que, en muchos casos, son irreparables.

Por esta razón, es fundamental no solo formular y establecer estrategias de contención efectivas, si no también tener una comprensión general de todos los elementos normativos y contractuales que abordan una violación en los sistemas y redes informáticas de una empresa. Esta visión permitirá a los responsables de la ciberseguridad convertir los escenarios evaluados en las diferentes fases del seminario "Equipos estratégicos en ciberseguridad: Red team & Blue team" en herramientas para establecer metodologías de intrusión como un instrumento que contribuya al fortalecimiento de la seguridad en los activos de información.

Este informe aborda temas como el marco regulatorio, el pentesting, intrusión y estrategias de contención, explorando su aplicación práctica y su relevancia ética y legal en el entorno actual de ciberseguridad para la empresa propuesta en el banco de trabajo practico “HackerHouse”.

[1] CCIT; IA Para la protección y prevención de amenazas; [Sitio web]; Desconocida; [Consulta: 19 marzo del 2024]; Disponible en: https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Fortalecer la postura de ciberseguridad de "HackerHouse" mediante el análisis del marco regulatorio, intrusión, pentesting, la evaluación de los equipos de respuesta y defensa, y la implementación de estrategias efectivas para el manejo y contención de ataques cibernéticos

1.2 OBJETIVOS ESPECÍFICOS

Comprender el funcionamiento, arquitectura y generalidades de las herramientas de seguridad informática para las pruebas de penetración.

Analizar el marco ético y regulatorio para determinar las responsabilidades de los ejercicios de Red Team y Blue Team del banco de trabajo.

Demostrar la existencia de vulnerabilidades en un sistema informático específico mediante la aplicación de metodologías y técnicas de intrusión, con el propósito de evaluar la identificación de riesgos e impactos de los incidentes de seguridad.

Formular estrategias de contención efectivas contra el incidente de seguridad expuesto en el banco de trabajo del seminario.

2 DESARROLLO DEL INFORME TÉCNICO

2.1 ETAPA 1: FUNDAMENTOS DE EQUIPOS DE SEGURIDAD

En esta primera etapa, se busca fortalecer las competencias en seguridad informática mediante:

- El análisis del marco regulatorio colombiano.
- La aplicación de pruebas de penetración (pentesting).
- La utilización de herramientas de Metasploit.

2.1.1 LA SEGURIDAD INFORMÁTICA EN COLOMBIA: ANÁLISIS COMPARATIVO ENTRE LA LEY 1273 DE 2009 & LA LEY 1581 DE 2012

La Ley 1273 de 2009 surge como una nueva herramienta legal para la protección de la información y los datos en Colombia. Esta ley modifica el Código Penal colombiano para tipificar los delitos informáticos y las sanciones correspondientes para cuando se atenta contra la confidencialidad, integridad y disponibilidad de la información, a continuación, se resumen los artículos que la componen:

- Artículo 1 Enmienda el Código Penal de Colombia para incorporar nuevas categorías de delitos vinculados a la informática.

- Artículo 269A Acceso no autorizado a un sistema informático: Se produce cuando alguien, sin permiso o excediendo los límites establecidos, ingresa a un sistema informático protegido.

- Artículo 269B Sabotaje ilícito de un sistema informático o red de telecomunicaciones: Se produce cuando alguien, sin autorización, interfiere o dificulta el funcionamiento habitual de un sistema informático o una red de comunicaciones.

- Artículo 269C Intercepción de datos informáticos: Sucede cuando alguien, sin permiso, intercepta o captura datos informáticos mientras se transmiten, almacenan o procesan en un sistema informático.

- Artículo 269D Daño informático: Se presenta cuando una persona, de manera intencionada y sin autorización, causa daño o deterioro a un sistema informático, a sus datos o a sus programas.

- Artículo 269E Uso de software malicioso: Corresponde cuando una persona, de manera intencionada y sin autorización, utiliza un programa informático diseñado para causar daño o perjuicio a un sistema informático, a sus datos o a sus programas.

- Artículo 269F Violación de datos personales: Se configura cuando una persona, sin autorización o excediendo los límites de esta, accede, intercepta, modifica, elimina o destruye datos personales contenidos en bases de datos, archivos o cualquier otro medio.

- Artículo 269G Suplantación de sitios web para capturar datos personales (phishing): Es un delito que se configura cuando una persona crea un sitio web falso que imita a un sitio web legítimo con el objetivo de engañar a los usuarios para que introduzcan sus datos personales.

- Artículo 269H Circunstancias de agravación punitiva: Corresponde a los factores que se tienen en cuenta para aumentar la pena de un delito cuando este se ha cometido de una manera especialmente grave.

- Artículo 269I Hurto por medios informáticos y semejantes: Se tipifica cuando un individuo, burlando las salvaguardias de seguridad informática, lleva a cabo una acción análoga al robo convencional (apropiarse de un objeto ajeno sin consentimiento), manipulando un sistema informático, una red electrónica, telemática u otro medio similar, o suplantando la identidad de un usuario frente a los sistemas de autenticación y autorización establecidos.

- Artículo 269J Transferencia no consentida de activos: Se configura cuando un individuo, con intención de obtener beneficios económicos y utilizando artimañas informáticas o métodos similares, logra la transferencia no autorizada de cualquier recurso en detrimento de otra persona.

- El Artículo 2° de la Ley 1273 de 2009 modifica el Código Penal colombiano para agregar una nueva circunstancia de mayor punibilidad: incrementando la pena de los delitos cuando se utilizan medios informáticos, electrónicos o telemáticos para su comisión.

- Artículo 3° Adición al Código de Procedimiento Penal del numeral 6 al artículo 37 donde se establece que los Jueces Penales Municipales conocen de los delitos contenidos en el Título VII Bis.

- Artículo 4° Establece que la ley entra en vigor desde su promulgación y anula cualquier norma que se oponga a ella.

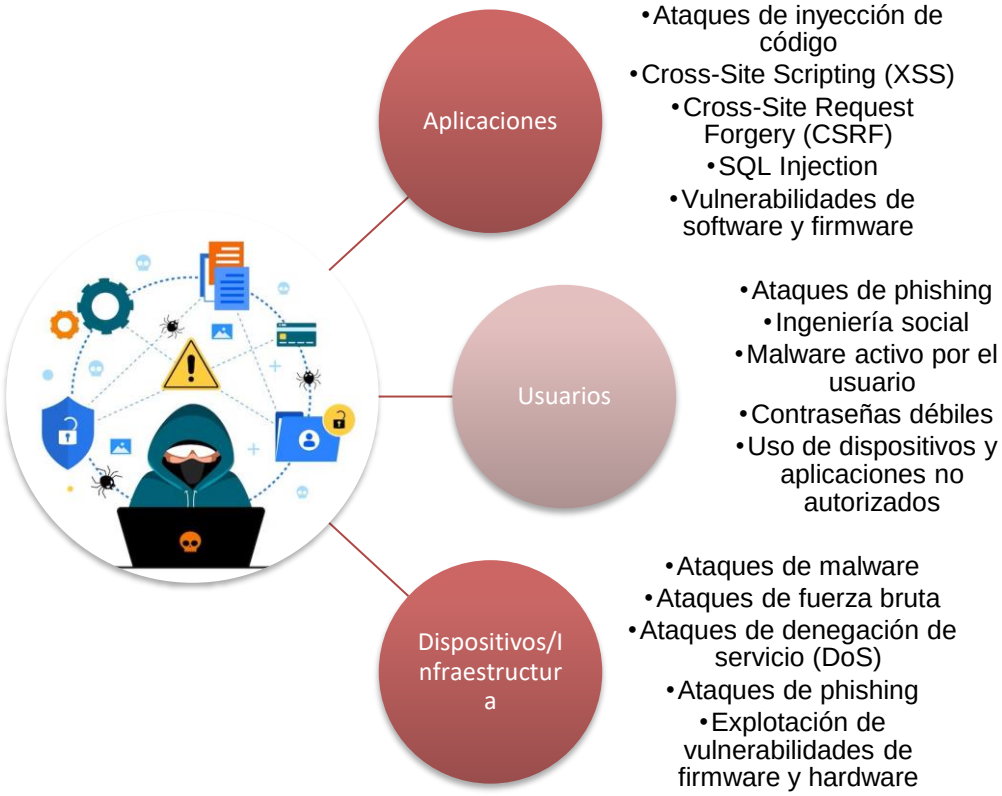
Por otra parte, la Ley 1581 de 2012 es una norma regulada por la Superintendencia de Industria y Comercio (SIC), debido a que establece los principios, deberes y derechos para el manejo de la información personal (tratamiento de datos). Esto abarca desde la recolección, almacenamiento, uso, circulación hasta la supresión de esta. En otras palabras, busca proteger el derecho a conocer, actualizar y rectificar toda aquella información nuestra recolectada en bases de datos, tanto comerciales como públicas y privadas.

Las sanciones por no cumplir con esta normativa pueden alcanzar hasta 1.000 salarios mínimos legales mensuales vigentes (SMMLV).

2.1.2 METODOLOGÍA DE PENTESTING: ANÁLISIS PARA LA DETECCIÓN DE VULNERABILIDADES

El Pentesting, también conocido como prueba de penetración, es una simulación de ataque cibernético a un sistema informático, red o aplicación. Y se desarrolla con el propósito de identificar vulnerabilidades que puedan ser explotadas por actores malintencionados.

Figura 1. Vectores de ataque conocidos en ejercicios de Hacking



Fuente: Autor

Etapa 1: Reconocimiento, Durante esta fase se realizan distintas actividades de reconocimiento (pasivo/activo) del objetivo que pueden generar valor para planear diferentes formas de ataque a partir de la comprensión de su operación y entorno.

El reconocimiento pasivo o Footprinting es aquel que no deja rastros de información en la red sobre los elementos capturados. Es decir, no se interactúa de forma directa con los sistemas para recolectar datos. Un ejemplo de esto es la información pública como nombre de empleados, cargos, direcciones de correo, sitios web y más.

Las ventajas del Footprinting son:

- Reducción del riesgo de detección de actividad.
- Orientación de la prueba en los objetivos más relevantes o con mayores vulnerabilidades.
- Detección de vulnerabilidades escondidas.

Algunas herramientas Open Source y pagas para esta actividad son:

Herramientas Open Source

- Nmap: Escaneo de puertos, servicios, sistemas operativos y más
- Netdiscover: Descubrimiento de hosts en la red
- Whois: Búsqueda de información de dominio
- DNSrecon: Búsqueda de información de DNS
- Maltego: Recopilación y análisis de información

Herramientas Pagas

- Metasploit Pro: Suite de herramientas de pentesting
- Acunetix: Escáner de vulnerabilidades web
- Nessus: Escáner de vulnerabilidades
- Burp Suite: Proxy web para interceptar y modificar el tráfico HTTP

Por otro lado, el reconocimiento activo o Fingerprinting se caracteriza por dejar rastros digitales. Esto se debe a que son estas interacciones donde se analiza de forma directa el sistema o aplicación y, por lo general, se otorgan permisos para dicha actividad.

Etapa 2: Enumeración/Escaneo, En esta etapa se profundiza en el análisis inicial de los activos identificados en la etapa 1, buscando información

detallada y específica sobre las debilidades en activos de información o configuraciones del sistema a partir de un escaneo completo.

Etapa 3: Explotación, Con la recolección previa de información se establecen planes de ataque. Esto significa que se explotan las vulnerabilidades o configuraciones deficientes, según la priorización, para acceder al sistema/red y elevar privilegios que permitan el acceso a datos sensibles como cuentas, contraseñas, bases de datos, entre otros.

Etapa 4: Post-Explotación, Los pentesters registran todos los pasos que siguen durante el proceso de investigación y explotación. Es decir que se mantienen y consolidan los accesos obtenidos para la recopilación de información adicional desde la elevación de privilegios simulando un ataque real de forma controlada y supervisada.

Etapa 5: Informe, En esta etapa se consolida un informe que incluye todo el detalle de las técnicas utilizadas para penetrar el sistema/red. Además, se identifican y analizan las brechas o vulnerabilidades detectadas, con el fin de determinar las acciones que se deben tomar para su remediación.

Adicionalmente, el pentester puede ayudar a establecer las prioridades que la organización debe abordar de forma inmediata y proponer medidas de remediación.

Etapa 6: Limpieza y remediación, Al igual que en ataques reales, estas pruebas de penetración pueden dejar rastros digitales que podrían ser aprovechados por atacantes internos o externos. Por lo tanto, es de suma importancia eliminar los accesos y/o artefactos utilizados en la prueba.

2.1.3 CVE: METASPLOIT PARA PRUEBAS DE SEGURIDAD

Los CVE o Vulnerabilidades y Exposiciones Comunes conforman un sistema de identificación y catalogación de vulnerabilidades en software y hardware. Este sistema es mantenido y gestionado por la corporación MITRE, quienes generaron una base de datos de fallas identificadas por cualquier persona u organización en productos y/o servicios de tecnología, lo que permite mantener actualizaciones de seguridad de forma continua ya que los reportes vienen desde diferentes entidades.

Los CVE se componen de una identificación alfanumérica única que permite la referencia confiable sobre las vulnerabilidades, sus prioridades y sus posibles soluciones.

Ejemplo: CVE-AAAA-NNNN:

- AAAA: Año de la publicación (por ejemplo 2024)
- NNNN: Número secuencial único asignado a la vulnerabilidad

De manera similar, la URL https://www.exploit-db.com/ nos redirige al sitio web de Exploit-DB, una biblioteca pública de información sobre vulnerabilidades de seguridad informática que fomenta la investigación y colaboración sobre exploits y técnicas relacionadas con el aprovechamiento de fallas de software o hardware.

Se relaciona con CVE, ya que cada exploit de esta base de datos está relacionado con uno o más CVE, lo que permite la búsqueda asertiva y eficiente de exploits para la explotación de la vulnerabilidad descrita en el

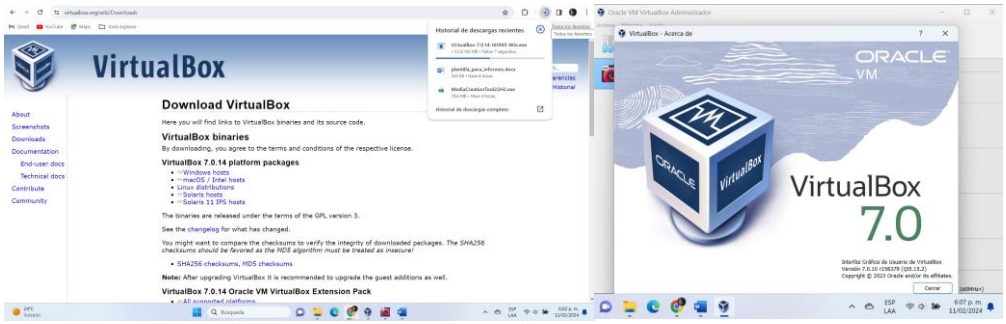
CVE. Por lo tanto, también facilita el análisis sobre la severidad de la vulnerabilidad en el sistema informático en caso de su explotación.

- Análisis de registros de red
- Conversación con el usuario afectado
- Detener el proceso o servicio desconocido
- Actualizar el estado de seguridad del componente
- Habilitar un programa de capacitación al área del recurso afectado o a la organización en general

2.1.4 DESARROLLO BANCO DE TRABAJO

Paso A Descargar la herramienta virtualizadora "VirtualBox" en su última versión:

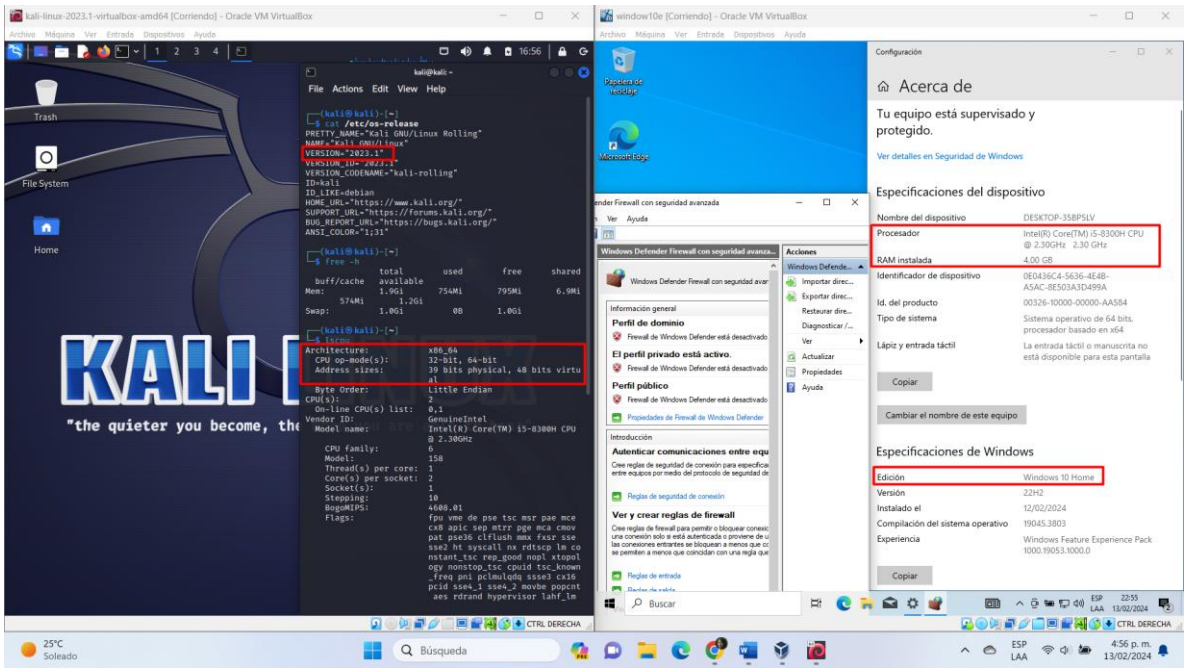
Figura 2. Instalación cliente VirtualBox 7.0



Fuente: El autor

Paso B Para el banco de trabajo se necesitan 2 máquinas virtuales: una con Kali Linux y la otra con Windows 10, deshabilitando completamente su sistema de seguridad (incluyendo Windows Defender, antivirus y firewall, entre otros).

Figura 3. Verificación de operación las máquinas virtuales Kali Linux & Windows 10



Fuente: El autor

Para este banco de trabo se desplegaron dos máquinas virtuales con las siguientes características:

Máquina Kali Linux

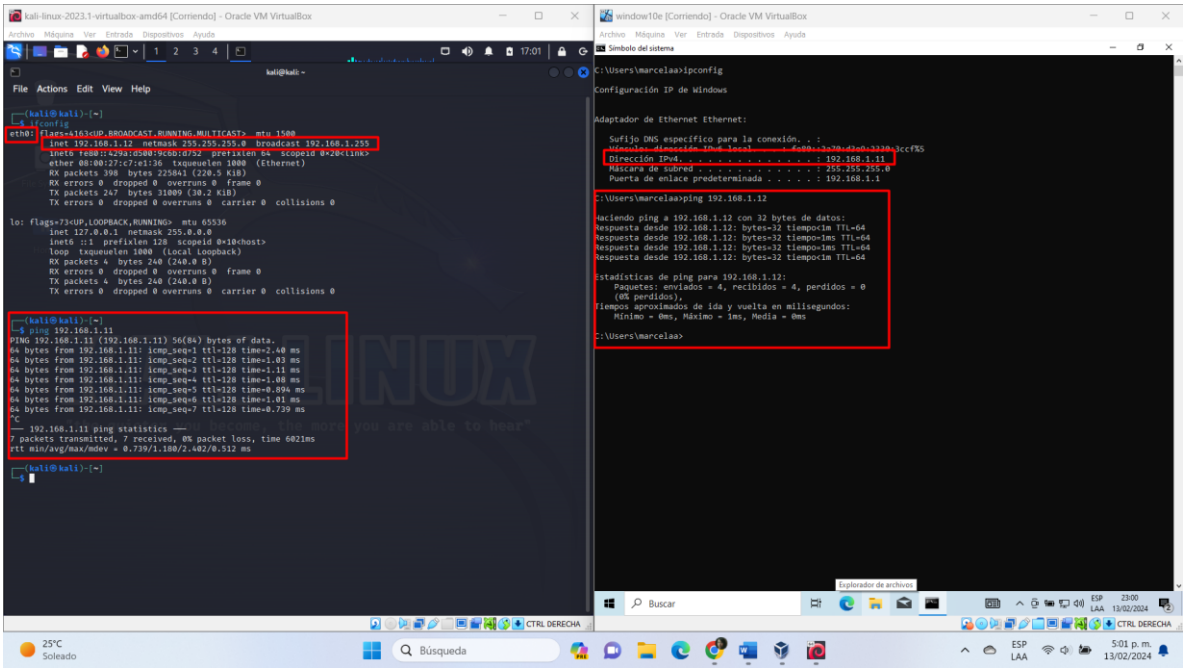
- Procesador: Intel Core i5
- Memoria RAM: 8 GB
- Almacenamiento: SSD de 256 GB
- Monitor: 15.6 pulgadas

- Teclado y ratón: Estándar

Máquina Windows 10

- Procesador: Intel Core i5
- Memoria RAM: 4 GB
- Almacenamiento: HDD de 500 GB
- Monitor: 14 pulgadas
- Teclado y ratón: Estándar

Figura 4. Prueba de comunicación de la infraestructura desplegada



Fuente: El autor

En la prueba de comunicación, no se llevaron a cabo configuraciones adicionales en la red de las dos máquinas virtuales. La prueba resultó exitosa debido a que, en VirtualBox, ambas máquinas están configuradas para

comunicarse a través de la tarjeta inalámbrica de la estación anfitriona en modo puente.

2.2 ETAPA 2: RESPONSABILIDADES ETICAS Y LEGALES

En la segunda fase, se analiza el desempeño de los equipos de Respuesta a Incidentes y Defensa de la Infraestructura en el escenario de estudio. El propósito de esta evaluación es asegurar la responsabilidad legal y ética de los profesionales de la Ciberseguridad en HackerHouse.

2.2.1 EVALUACIÓN DEL ACUERDO DE CONFIDENCIALIDAD: ARGUMENTADO SEGÚN EL MARCO NORMATIVO COLOMBIANO

¿Qué secciones del acuerdo de confidencialidad considera usted que podrían ser consideradas como contrarias a la ley?

En el anexo 2, titulado "Escenario 2", se destaca que la empresa HackerHouse figura entre las mejores compañías a nivel mundial en ciberseguridad. Esta posición sugiere que sus principios se basan en cumplir con las leyes y regulaciones de cada país donde opera, con el objetivo de proteger la información confiada, fomentar la confianza y promover una competencia justa al actuar con responsabilidad contractual.

No obstante, al revisar los párrafos del anexo 3, se identifican algunas inconsistencias con las buenas prácticas legales. Es importante abordar estas

discrepancias para garantizar la integridad y la ética en las operaciones de la empresa:

- Primera clausula "*La información sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados"*

  Esta porción de texto en la cláusula se considera ilegal, ya que obliga al receptor a mantener silencio sobre actividades ilícitas. Esto contraviene el artículo 309 de la ley, que se refiere a la "obstrucción a la justicia"[2]. Además, va en contra del derecho a la información establecido en el artículo 24 de la ley 1271, así como de la libertad de expresión. Es importante revisar y modificar esta cláusula para asegurar su conformidad con las leyes y principios éticos.

- Segunda clausula, enciso #2 *"Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos""*

  se resalta la información relacionada con "datos de chuzadas, interceptación ilegal de información y accesos abusivos a sistemas informáticos". Esto se considera una infracción de la Ley 1708 de 2014, específicamente en el artículo 167. Además, se viola el código penal, en particular el artículo 269A, lo que afecta la privacidad e intimidad tanto de personas como de organizaciones

[2] LEYES; Código de Procedimiento Penal. Artículo 309; [Sitio web]; Bogotá, Colombia; [Consulta: 17 febrero del 2024]; Disponible en: https://leyes.co/codigo_de_procedimiento_penal/309.htm

- Cuarta clausula, enciso #3 *"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros"*

  Destaca el hecho de que imposibilitar al receptor a establecer denuncias sobre los delitos que puedan surgir en el ejercicio de sus actividades podría considerarse como complicidad en actividades ilícitas. Además, esta acción va en contra de la Ley 1273 de 2009, específicamente en los artículos 269ª, 269F y 269J. Asimismo, contraviene la Ley 1581 de 2012 (Protección de Datos Personales), en particular los artículos 4, 8 y 17, al obstaculizar el deber ciudadano y profesional de denunciar hechos delictivos

- Cuarta clausula, enciso #6 *"La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse"*

  Este fragmento de la cláusula establece un "pacto de silencio" con el receptor. Dicho pacto impide al receptor, desde su perspectiva moral personal y profesional, ejercer su derecho a la denuncia. Esto aplica especialmente en situaciones donde sus funciones exceden los límites legales y afectan a personas u organizaciones[3].

[3] CONGRESO DE LA REPÚBLICA; Ley 906 Por la cual se expide el Código de Procedimiento Penal; [Sitio web]; Bogotá, Colombia; [Consulta: 18 febrero del 2024]; Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_09060_204a_pr001.html#67

- Cuarta clausula, #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"*

  Esta cláusula tiene como objetivo responsabilizar al receptor por la información que no le pertenece. Dicha acción se considera una forma de coacción, ya que impide que el receptor colabore con las autoridades competentes. Esto afecta su derecho a la defensa y al debido proceso, tal como se establece en la Sentencia T-018/17 [4].

- Sexta clausula, *"La parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas"*

  Esta cláusula podría considerarse ilegal debido a que establece una responsabilidad civil contra el receptor sin justa causa por malas prácticas de la empresa. Esta acción se considera un abuso del colaborador, ya que va en contra de la Sentencia C-822 (2005), específicamente en el artículo 3, que establece el principio de proporcionalidad en el Código Penal colombiano[5]

[4] CORTE CONSTITUCIONAL; Acción de tutela contra providencias judiciales-Reiteración de jurisprudencia sobre procedencia excepcional; [Sitio web]; Bogotá, Colombia; [Consulta: 18 febrero del 2024]; Disponible en: https://www.corteconstitucional.gov.co/relatoria/2017/t-018-17.htm

[5] ARIAS, D; Proporcionalidad, pena y principio de legalidad; [Sitio web]; Barranquilla: UDA; [Consulta: 18 febrero del 2024]; Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972012000200005#:~:text=El%20art%C3%ADculo%203%20del%20CP,de%20necesidad%2C%20proporcionalidad%20y%20razonabilidad.

- Octava clausula *"En caso de 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 párrafo podría considerarse ilegal debido a la coerción ejercida sobre el receptor, lo que nuevamente obstaculiza su deber personal y profesional de denunciar actividades ilegales en el ejercicio de sus funciones. Además, es relevante señalar que la responsabilidad legal y penal no puede transferirse de una empresa a su empleado o a cualquier otra persona, ya que esto podría considerarse un procedimiento inválido al infringir el cumplimiento de la Sentencia C-025 (2009), que garantiza el derecho a la defensa y al debido proceso[6].

- Novena clausula *"Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas"*

  Dado que la empresa no limita sus servicios al territorio colombiano, el acuerdo debería especificar que su aplicación y validez estarán sujetas al país donde se lleve a cabo la actividad o relación comercial. Esto es relevante para garantizar que los derechos de los clientes y empleados estén protegidos según las leyes de su propio país.

[6] CORTE CONSTITUCIONAL; Acción de tutela contra providencias judiciales-Reiteración de jurisprudencia sobre procedencia excepcional; [Sitio web]; Bogotá, Colombia; [Consulta: 18 febrero del 2024]; Disponible en: https://www.corteconstitucional.gov.co/relatoria/2017/t-018-17.htm

2.2.2 RESPUESTA A LA PREGUNTA GENERADORA: ¿ACEPTARIA EL CONTRATO Y EL ACUERDO DE CONFIDENCIALIDAD, DONDE SE PUEDEN ENCONTRAR PROCESOS ILEGALES?

Se rechazaría la oferta laboral después de analizar el anexo 2 y el anexo 3 de la empresa HackerHouse. En estos documentos, encontró no solo inconsistencias legales, sino también una grave falta de ética profesional por parte de los responsables de la organización al proponer una relación laboral con engaños. Estos engaños podrían conllevar medidas disciplinarias por parte del COPNIA al incumplir los siguientes artículos de su código de ética:

Articulo 31 Principios generales de la práctica profesional, establece que los profesionales tienen el deber de:

- Cuidar los bienes que se les entreguen en función de sus labores, impidiendo su destrucción, ocultamiento o uso indebido.
- Informar sobre las transgresiones al código de ética que observen en el ejercicio de su profesión.
- Ser colaboradores y transparentes con los elementos probatorios que tenga a su disposición.

Articulo 32 Limitaciones generales para el ejercicio profesional:

- No consentir, admitir o propiciar la usurpación de funciones profesionales tipificadas en la ley

Articulo 34 Restricciones específicas para los profesionales en relación con la sociedad:

- Aceptación de trabajos que vayan yendo en contra de lo establecido por la ley

Articulo 35 Obligaciones de los profesionales para con el decoro de sus oficios:

- Respectar y velar porque se respete la ley y reglas que inciden en los actos de la profesión, por lo cual se deben denunciar todas sus transgresiones

- Velar por el buen nombre y prestigio de la profesión

Artículo 39. Deberes de los profesionales para con sus clientes y el público en general:

- Mantener la confidencialidad de toda información relacionada con clientes y sus colaboradores, sin embargo, cuando se incumplimiento de la ley se debe atender la obligación legal de revelarla mediante una denuncia.
- Ser guardianes de los intereses de los clientes, por lo que no es legal actuar en su perjuicio

Articulo 53 Cancelación de la licencia profesional:

- Obstaculizar investigaciones del consejo profesional de ingeniería
- Cometer delitos que impacten a clientes, colegas o autoridades

- Cualquier violación a los deberes, obligaciones y prohibiciones establecidas en el código de ética de COPNIA y la ley 1482 del 2003

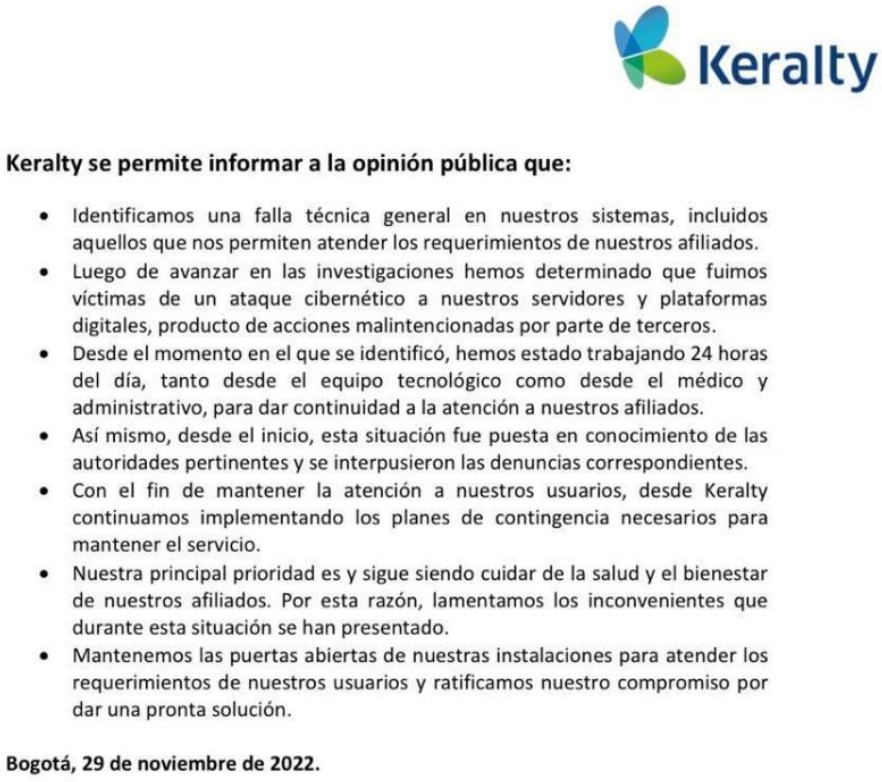
2.2.3 ATAQUE CIBERNETICO EPS SANITAS Y COLSANITAS: RANSOMWARE

El 29 de noviembre del año 2022, el grupo Keralty anunció públicamente que fue víctima de un ataque de ciberseguridad que provocó diferentes fallas en la operación de sus plataformas de servicios virtuales. Como primera instancia, activaron sus mecanismos de contingencia y dieron parte a las autoridades competentes para la denuncia del hecho.[7]

Según iTechSAS (2022) "la Superintendencia reportó que, desde que se conoció la contingencia de la EPS, los usuarios han formulado 10.455 peticiones, quejas y reclamos, de los cuales 7.442 aún se encuentran en gestión por parte de la entidad promotora de servicios de salud".

[7] MINTIC; En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia; [Sitio web]; Bogotá, Colombia; [Consulta: 20 febrero del 2024]; Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

Figura 5. Comunicado oficial del grupo Keralty – Incidente de Ciberseguridad



Keralty

Keralty se permite informar a la opinión pública que:

- Identificamos una falla técnica general en nuestros sistemas, incluidos aquellos que nos permiten atender los requerimientos de nuestros afiliados.
- Luego de avanzar en las investigaciones hemos determinado que fuimos víctimas de un ataque cibernético a nuestros servidores y plataformas digitales, producto de acciones malintencionadas por parte de terceros.
- Desde el momento en el que se identificó, hemos estado trabajando 24 horas del día, tanto desde el equipo tecnológico como desde el médico y administrativo, para dar continuidad a la atención a nuestros afiliados.
- Así mismo, desde el inicio, esta situación fue puesta en conocimiento de las autoridades pertinentes y se interpusieron las denuncias correspondientes.
- Con el fin de mantener la atención a nuestros usuarios, desde Keralty continuamos implementando los planes de contingencia necesarios para mantener el servicio.
- Nuestra principal prioridad es y sigue siendo cuidar de la salud y el bienestar de nuestros afiliados. Por esta razón, lamentamos los inconvenientes que durante esta situación se han presentado.
- Mantenemos las puertas abiertas de nuestras instalaciones para atender los requerimientos de nuestros usuarios y ratificamos nuestro compromiso por dar una pronta solución.

Bogotá, 29 de noviembre de 2022.

Fuente: iTechSAS (2022)

Este incidente dio como resultado la pérdida confirmada de 0,7 terabytes de datos tras la ejecución de un ransomware por parte del grupo RansomHouse, que hizo también pública información de estados financieros, balances e información personal para ejercer presión al pago del rescate, según se reportó en VMware ESXi.

¿Qué implicaciones éticas y legales se comprometieron en este ataque Cibernético?

- Violación de la Ley 1581 de 2012 (Seguridad de Datos Personales): Como resultado del ataque, el grupo Keralty debió informar de primera

mano a los usuarios sobre la afectación que se podría presentar y se presentó frente a la prestación de sus servicios y la continuidad del negocio, así como también las medidas reactivas que se implementaron para proteger sus datos.

- Violación de la Ley 1273 de 2009 (Habeas Data): Debido a la pérdida de la información interna y externa (usuarios), el grupo Keralty puede enfrentarse a una penalización contractual por parte de la SIC debido al impacto que se puede presentar por la pérdida de datos personales de sus usuarios.

- Artículo 269A Intrusión no autorizada en un sistema informático: Ocurre cuando un individuo, sin permiso o yendo más allá de lo permitido, ingresa a un sistema informático que está protegido

- Artículo 269B Perturbación no autorizada de un sistema informático o red de telecomunicaciones: Se produce cuando un individuo, sin tener la potestad para ello, obstruye o entorpece el correcto funcionamiento de un sistema informático o una red de telecomunicaciones.

- Artículo 269E Uso de software malicioso: Se produce cuando un individuo, de manera intencionada y sin permiso, emplea un programa informático creado para ocasionar daño o perjuicio a un sistema informático, a la información que este contiene o a sus programas.

- Artículo 269F Exposición de datos personales: Se produce cuando un individuo, sin permiso o yendo más allá de lo permitido, accede, intercepta, modifica, elimina o destruye información personal contenida en bases de datos, archivos o cualquier otro medio.

- Artículo 269J Transferencia no consentida de activos: Ocurre cuando un individuo, con el objetivo de obtener un lucro personal y valiéndose de algún tipo de manipulación informática o técnica similar, consigue la transferencia no consentida de cualquier activo, perjudicando a un tercero.

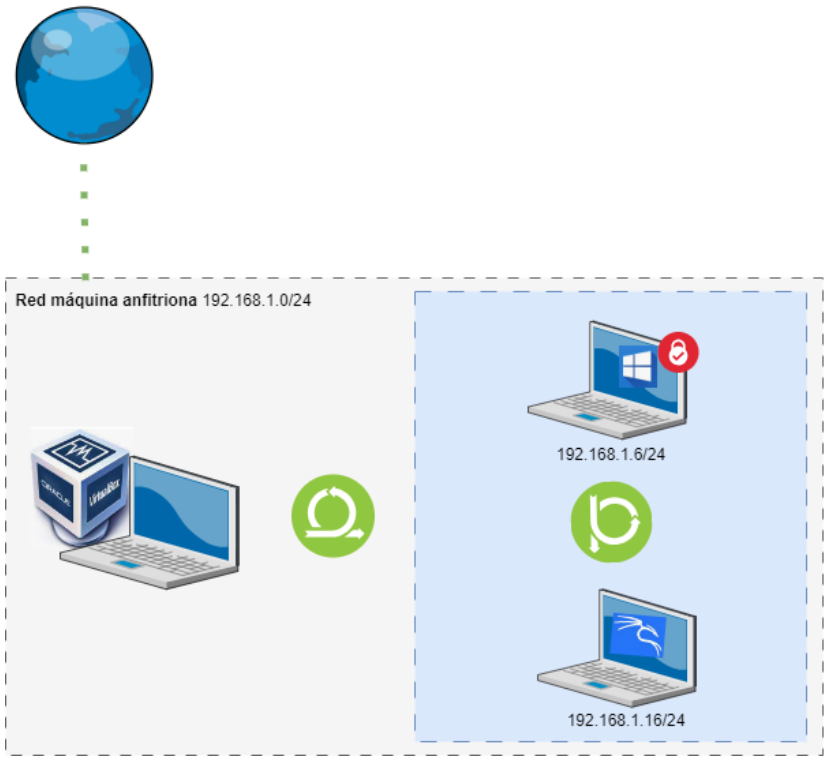
- Transgresión del Código Penal Colombiano: Los responsables de este ataque cibernético podrían ser procesados y condenados con hasta noventa meses de cárcel y/o multas que van entre los cien y los mil salarios mínimos legales vigentes en Colombia.

2.3 ETAPA 3: EXPLORANDO VULNERABILIDADES & EJECUTANDO PRUEBAS DE INTRUSIÓN

La etapa tres tiene como objetivo validar la presencia de debilidades en un sistema informático particular mediante la aplicación de enfoques y tácticas de intrusión para aprovechar las deficiencias en la red y la infraestructura de "HackerHouse".

2.3.1 EVALUACIÓN RECURSOS INFORMATICOS (SOFTWARE) EMPLEADO PARA EL DESARROLLO DEL ANEXO 4 – ESCENARIO 3: REDTEAM

Figura 6. Diagrama de infraestructura escenario 3 – Entorno de trabajo



Fuente: El autor

A continuación, se resumen las capacidades técnicas a nivel de herramientas de software empleadas para el desarrollo del ejercicio Red Team en la arquitectura de la figura 1.

- La máquina anfitriona debe contar con la capacidad de recursos suficientes para el aprovisionamiento de máquinas virtuales

- Herramienta de virtualización VirtualBox

- Servidor virtual Kali Linux: Maquina que simulara el atacante

- Servidor Virtual Windows 10: Maquina que simulara el objetivo

- NMAP: Herramienta de escaneos a la red para búsqueda de vulnerabilidades o fallas que puedan ser explotadas en auditorias de seguridad

- Msfvenom: Herramienta para la creación de payloads maliciosos en diferentes formatos, incluyendo ejecutables (.exe)

- Metasploit: Framework de código abierto para pruebas de penetración y análisis de vulnerabilidades.

- Meterpreter: Shell reversa que permite controlar de forma remota la máquina víctima.

2.3.2 ANÁLISIS DE DATOS PARA DETECTAR VULNERABILIDADES EN LA MÁQUINA ATACADA EN EL ESCENARIO 3 DEL ANEXO 4

Al analizar el escenario descrito en el anexo 4, se puede concluir que la raíz del problema de pérdida y filtración de información radicó en la falta de medidas de seguridad para proteger los datos almacenados en la máquina o estación de trabajo. Además, la insuficiente capacitación del empleado en las mejores prácticas de ciberseguridad también contribuyó al incidente. A continuación, se presentan los aspectos críticos de las conclusiones alcanzadas por el equipo de Red Team durante la revisión con el usuario afectado:

- Uso de aplicaciones no corporativas para la comunicación interna (por ejemplo, WhatsApp Web): Se identificó que algunos empleados utilizan aplicaciones no autorizadas para la comunicación interna, lo que podría representar un riesgo de seguridad.

- Ausencia de controles de línea base: No se aplicaron controles esenciales para monitorear y mantener el estado saludable de las máquinas. Estos controles incluyen antivirus, reglas de firewall, monitoreo y actualizaciones. Durante el análisis, se encontró que estos controles estaban desactivados.

- Falta de controles para el manejo de información en las estaciones de trabajo: No se han implementado controles adecuados para supervisar y gestionar el flujo de información en las estaciones de trabajo de la empresa. Esto quedó evidenciado cuando un usuario descargó y ejecutó un archivo no autorizado en su estación de trabajo.

- Ausencia de controles para usuarios con roles de alto privilegio: Los permisos administrativos del sistema operativo en las estaciones de trabajo no están restringidos para usuarios con roles de alto privilegio. Esta falta de limitación aumenta el riesgo de daños causados por instalaciones o configuraciones no autorizadas. En este caso, el usuario realizó modificaciones en la configuración del software.

- Falta de control o monitoreo de conexiones laterales: No se ha implementado un sistema de monitoreo para detectar conexiones no autorizadas. Esto resultó en la filtración de información interna desde un

archivo .TXT que contenía datos de "Nombre_estudiante_codigo_fecha_actividad".

2.3.3 ANÁLISIS DE SEGURIDAD EN WINDOWS 10: IDENTIFICACIÓN DE FALLOS Y VULNERABILIDADES

En el contexto del ejercicio de Red Team, cuyo objetivo es analizar y explotar brechas de seguridad en el sistema o red objetivo, se llevó a cabo una evaluación específica en la máquina donde se produjo el incidente de seguridad en tres etapas:

- Recopilación de información general de la red.
- Escaneo de vulnerabilidades en la máquina objetivo.
- Obtención de información general y realización de una prueba básica de comunicación.

En la evaluación general, se logra identificar que el ataque de ciberseguridad fue un evento de fuga de información interna. En otras palabras, en el contexto del anexo 4, se plantea que el agresor tenía acceso a la red corporativa de la máquina objetivo y además estaba familiarizado con datos sobre el responsable de dicha máquina. A continuación, se describen los posibles pasos que se ejecutaron para escanear la red a partir de la IP asignada a la máquina Linux (atacante) con el fin de identificar y seleccionar el objetivo.

Paso 1: Se ejecuta una consulta local en la estación Kali Linux para identificar el segmento de red al que está conectada. Y a continuación con dicha información se identifican los hosts activos en la red mediante el comando

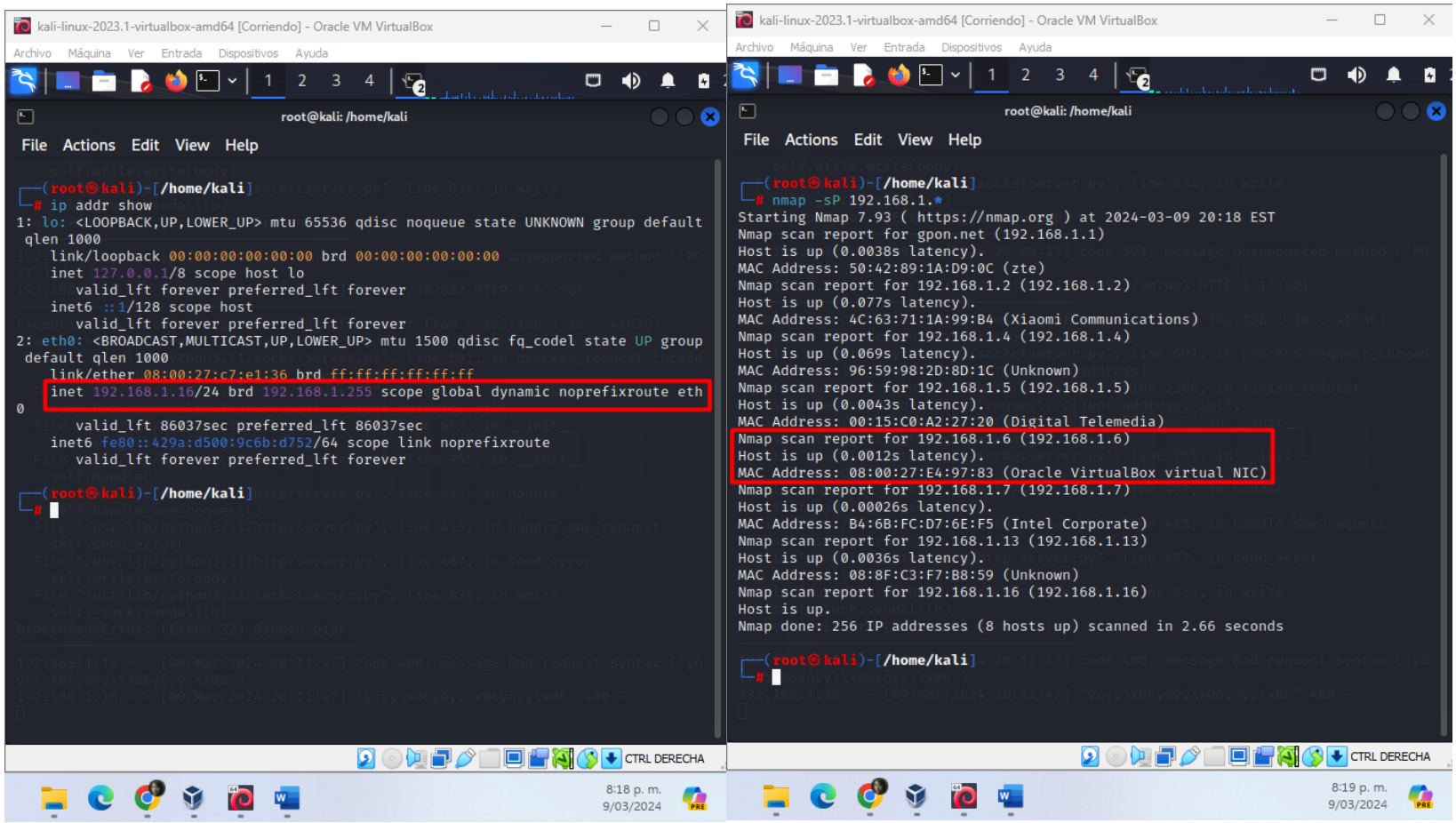
Nmap -sS 192.168.1.* y, de esta manera, establecer un objetivo favorable bajo los criterios puertos abiertos y máquinas activas (Figura 2).

Paso 2: Se lanza una petición de escaneo general a través del comando ***Nmap -O 192.168.1.**** (figura3) para obtener una imagen completa del host conectado a la red, puertos y servicios abiertos e información sobre sistema operativo y firewall. Esta información permitirá al atacante afinar su estrategia de explotación ya que dirigirá su esfuerzo a una brecha especifica.

Paso 3: Este último paso consiste en reconocer si existe o no un firewall o sistemas de seguridad perimetral que afecte la planificación del ataque. Este análisis previo proporciona información crucial que fortalece significativamente la estrategia del ataque y aumenta las posibilidades de éxito del mismo.

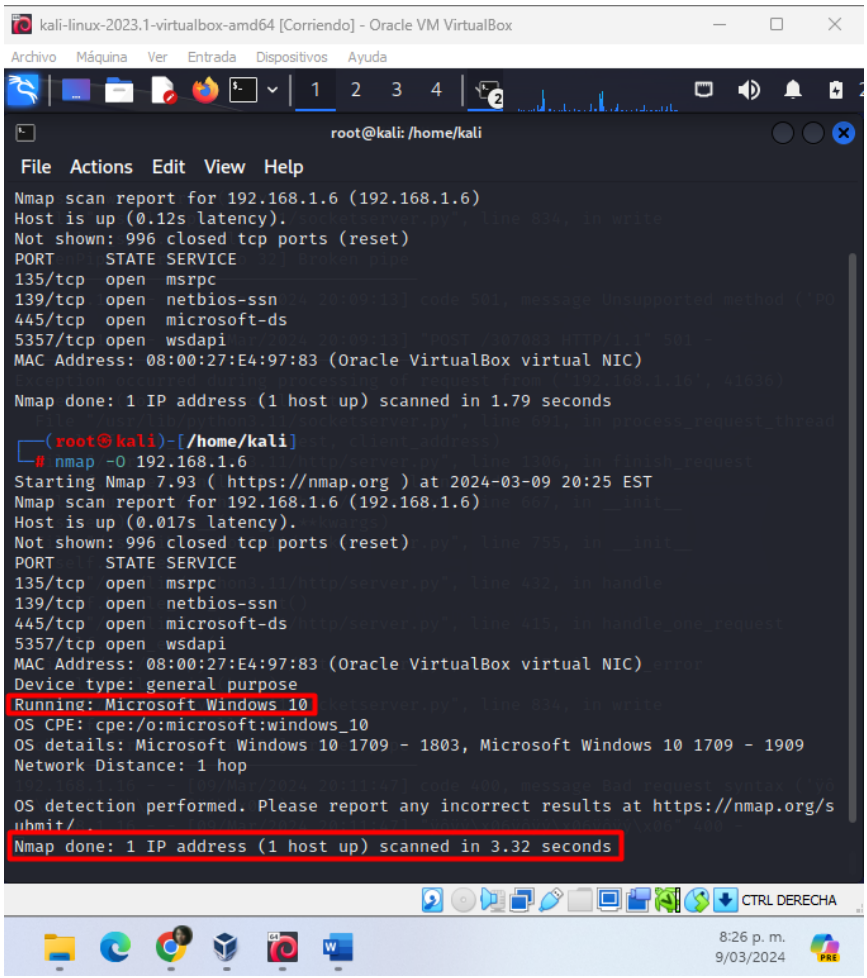
Detección: Esta fase monitorea la red y el sistema en búsqueda de actividad inusual, lo que será de ayuda para reconocer el tipo de ataque que está afectando el componente. Por ejemplo ¿Existen lentitud inusual, bloqueos, nuevos procesos, incrementos de consumo en los registros, entre otros?

Figura 7. Análisis de procesos y configuraciones base – PC Windows



Fuente: El autor

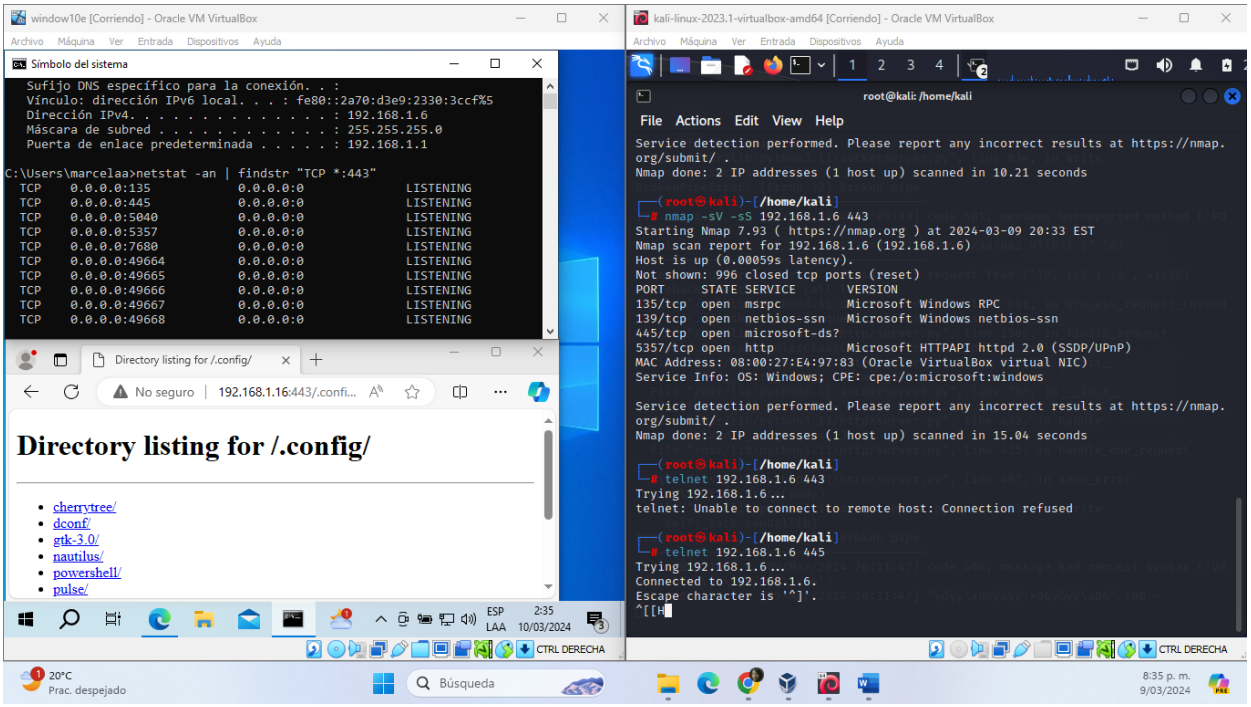
Figura 8. Escaneo de vulnerabilidades en la máquina objetivo



Fuente: El autor

Este escaneo proporciona un resumen de los servicios y puertos abiertos identificados por la herramienta, así como del sistema operativo de la IP seleccionada como víctima en esta prueba de seguridad. Es relevante mencionar que, aunque el servicio y el puerto 443 no aparecen en la lista resultante, no hubo problemas con su explotación debido a su naturaleza de uso, que es el tráfico HTTP.

Figura 9. Prueba de conexión con el puerto objetivo

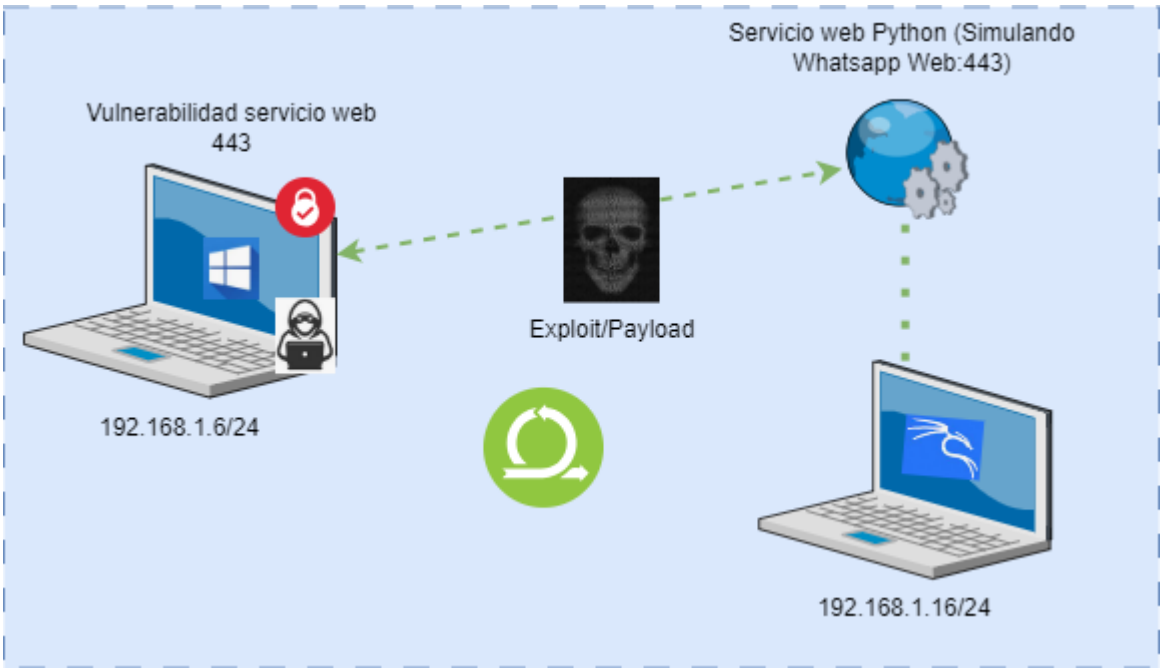


Fuente: El autor

Al igual que en el escaneo previo, la prueba de conexión del servicio Telnet en la IP y puerto configurados para el ataque resultó “no exitosa”. Sin embargo, se observó que la simulación de la descarga del archivo a través de WhatsApp Web (en nuestro caso de prueba, un sitio público con origen en la IP de Kali) por el puerto 443 sí tuvo éxito. Esto indica que el puerto 443 está abierto y disponible en la red, a pesar de no haber sido detectado ni en consultas locales (Windows) ni en los escaneos de Nmap realizados desde Kali Linux.

2.3.1 ANÁLISIS DE EXPLOIT EN WINDOWS 10: IDENTIFICACIÓN GRÁFICA DEL IMPACTO AL SISTEMA OPERATIVO

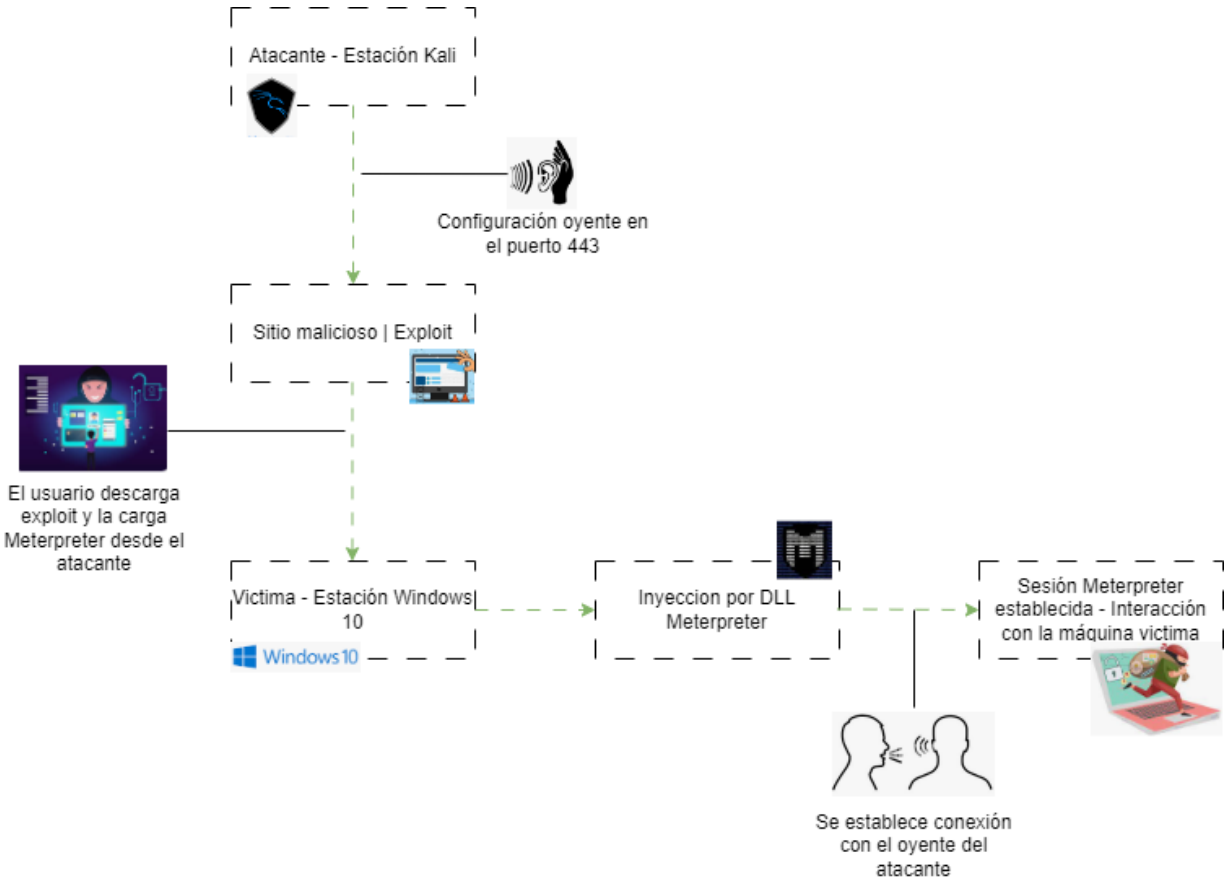
Figura 10. Explotación de meterpreter en Sistema operativo Windows 10



Fuente: El autor

El gráfico 5 ilustra cómo el atacante expuso el archivo infectado con el exploit a la estación víctima a través del servicio web, simulando el consumo de WhatsApp Web. En este caso, se cargó el exploit con el payload ***windows/x64/meterpreter/reverse_tcp*** para su descarga y ejecución, tal como se describe en el anexo 4.

Figura 11. Flujo de operación del ataque en Windows 10



Fuente: El autor

A continuación, se detalla a alto nivel cómo funciona el flujo de la figura 6:

Vulnerabilidad: Es una debilidad o fallo de seguridad que se pueden presentar desde el diseño, implementación o configuración de software, la cual de cierto modo no afecta al usuario final porque le es imperceptible pero que en ciertos escenarios permiten a un atacante el acceso a la red e infraestructura.

Exploit: Es un programa diseñado y usado para aprovechar una vulnerabilidad del sistema, es decir que se implementa en un ataque para producir fallos o errores en los servicios y operación mediante cargas de acciones o comandos.

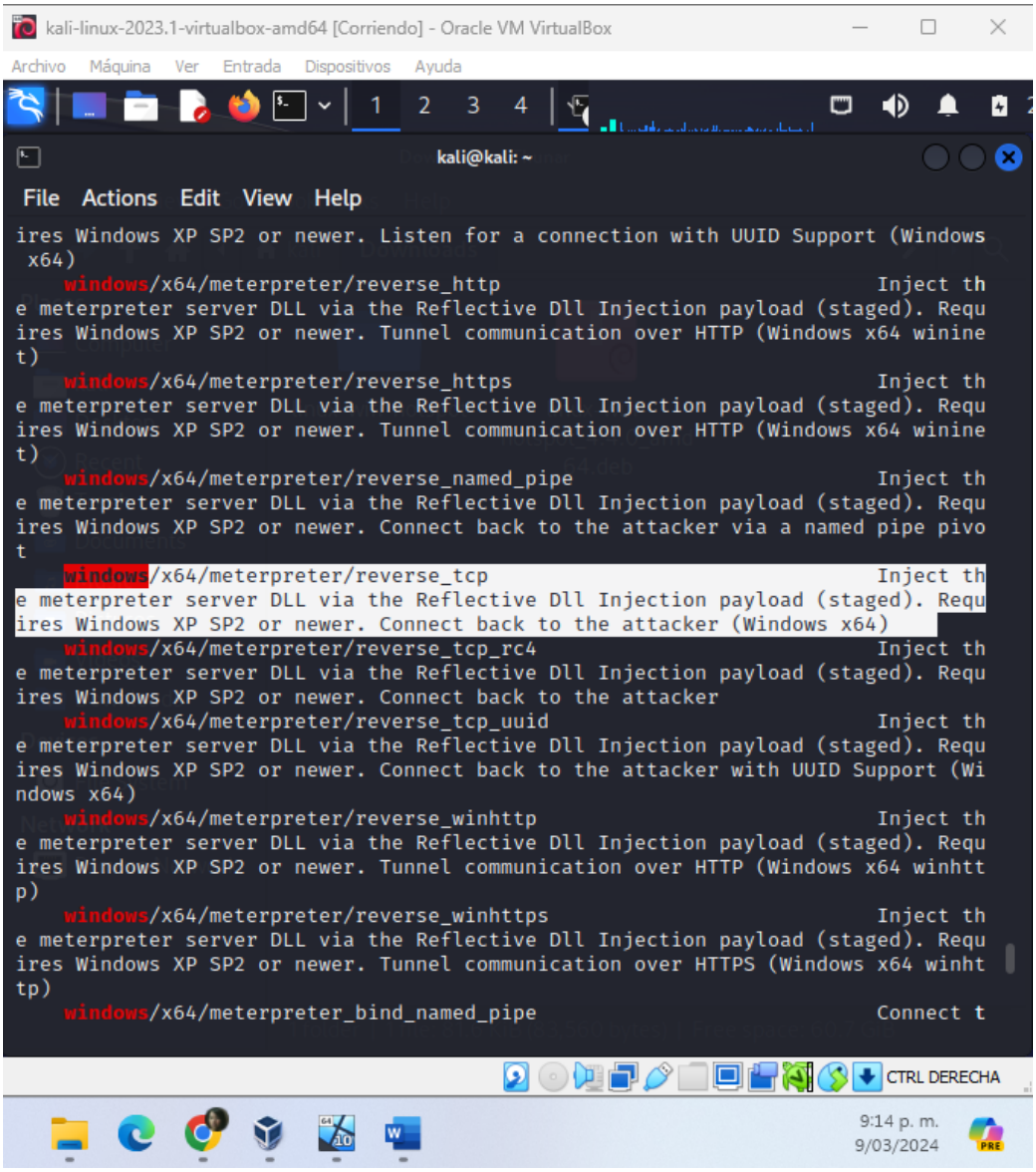
Payload: Es una carga de información que ejecuta o activa tras haber explotado la vulnerabilidad, es decir que aprovecha las fallas o errores abiertas por el exploit para ejecutar comandos o acciones que ataquen al sistema y su funcionamiento.

En el escenario se simulo la exposición web de un archivo infectado para que el usuario victima lo descargue y active la carga del exploit de forma local, lo cual le permite al atacante manipular y escalar sus privilegios para el robo de información.

Paso 1: Selección y construcción del Payload para el sistema operativo Windows 10, según las acciones del atacante (robo de información).

En este escenario, se llevó a cabo una búsqueda utilizando el comando ***msfvenom -l payloads | grep Windows***, que se enfoca en el sistema operativo para el cual se busca una carga útil. Se seleccionó la carga ***windows/x64/meterpreter/reverse_tcp***, que proporciona las instrucciones necesarias para lograr acceso remoto a un sistema operativo de 64 bits con fines de escalada de privilegios.

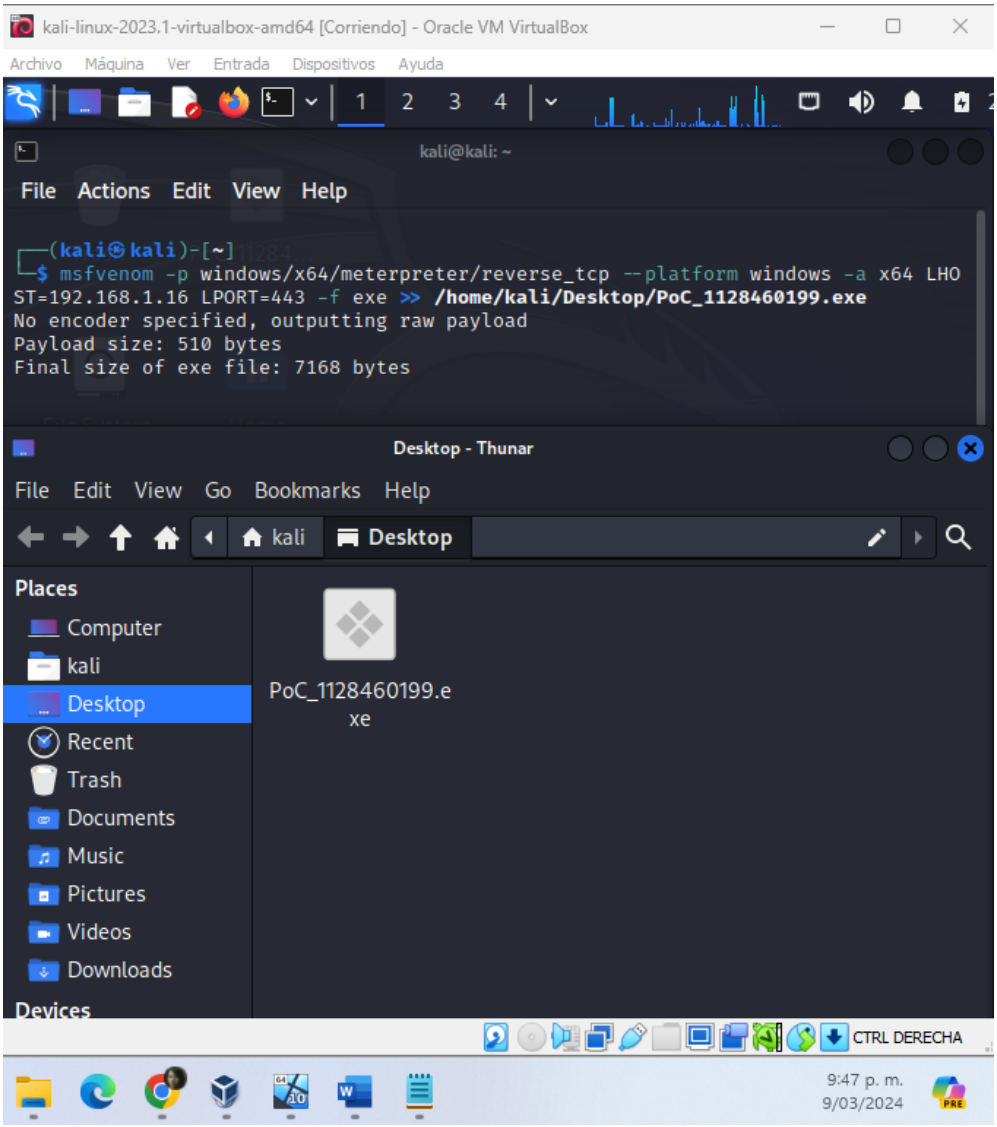
Figura 12. Búsqueda y selección de Payload



Fuente: El autor

Para la creación del payload de Metasploit, se eligió la carga windows/x64/meterpreter/reverse_tcp específica para la plataforma Windows de 64 bits. Este payload fue generado para la dirección IP del servidor atacante, utilizando el puerto 443, y se guardó en un archivo con formato .exe en el escritorio de este.

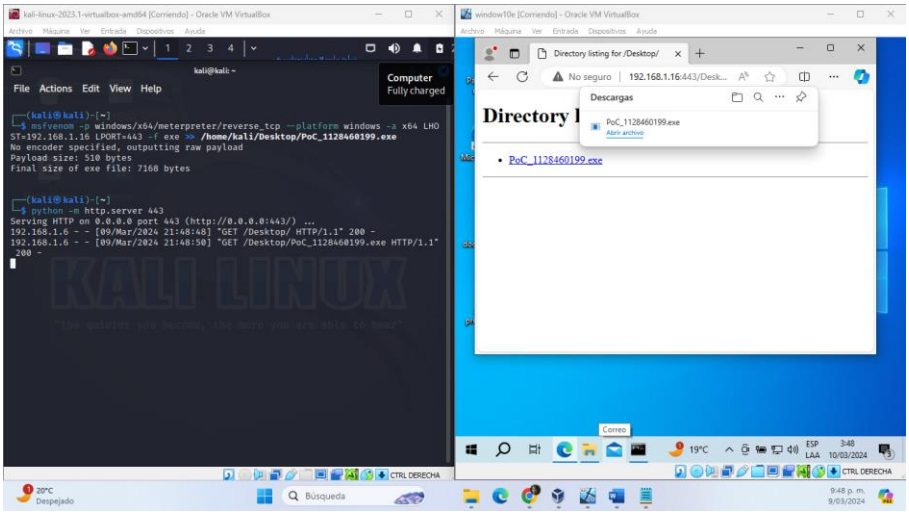
Figura 13. Construcción del Payload



Fuente: El autor

Paso 2: Se configuró un oyente en el puerto 443 para permitir la descarga y ejecución del documento PoC_1128460199.exe por parte de la víctima en una máquina con Windows 10. Esto simula la consulta y descarga del documento por parte del usuario que informó la pérdida de su información.

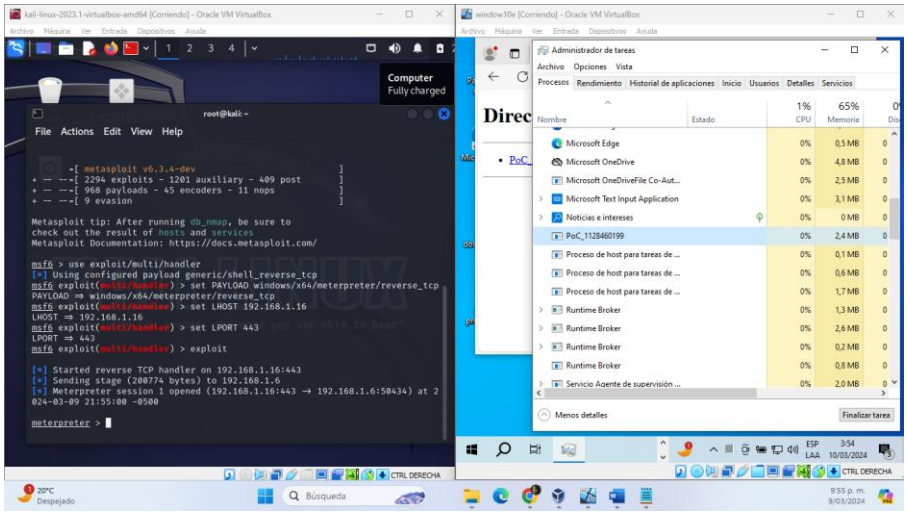
Figura 14. Habilitación servicio web | simulación consumo por WhatsApp Web



Fuente: El autor

Paso 3: Configuración y activación del exploit en modo escucha en la máquina atacante con los parámetros de IP y puerto configurado en el paso 1 y descarga e instalación del Payload en la máquina victima por el usuario afectado.

Figura 15. Configuración Exploit y activación de Payload



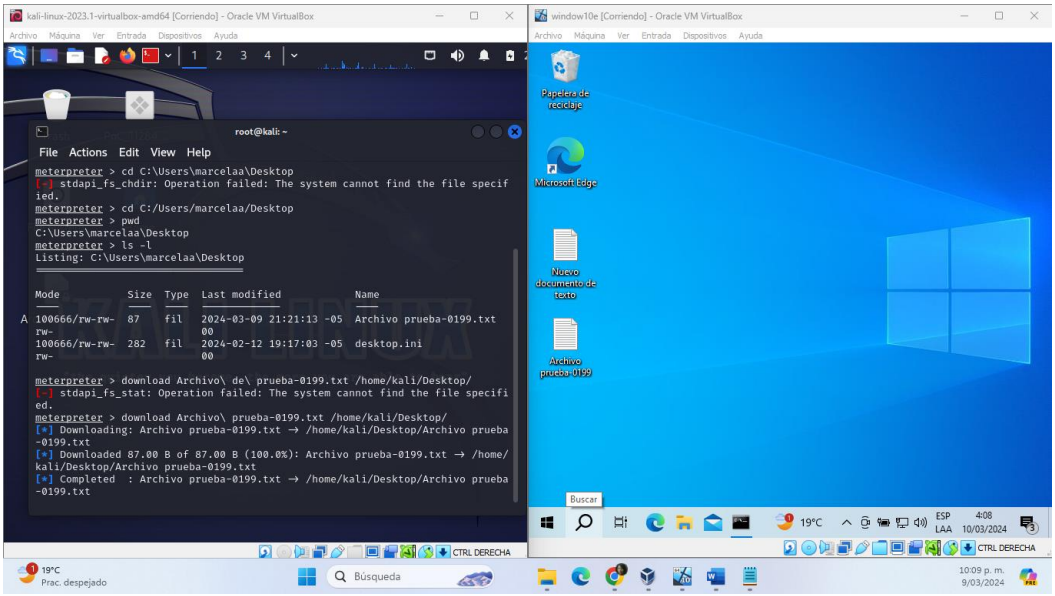
Fuente: El autor

Paso 4: Tras una instalación exitosa del payload por parte del usuario afectado, se habilitó el acceso en la máquina víctima para la escalación de privilegios y el robo de información por parte del atacante.

En este escenario, el atacante tiene como objetivo sustraer y eliminar el archivo "Archivo prueba-0199.txt". Para lograrlo, en la consola de Metasploit, se busca la ubicación del servidor de archivos o el "file Server" para ejecutar comandos.

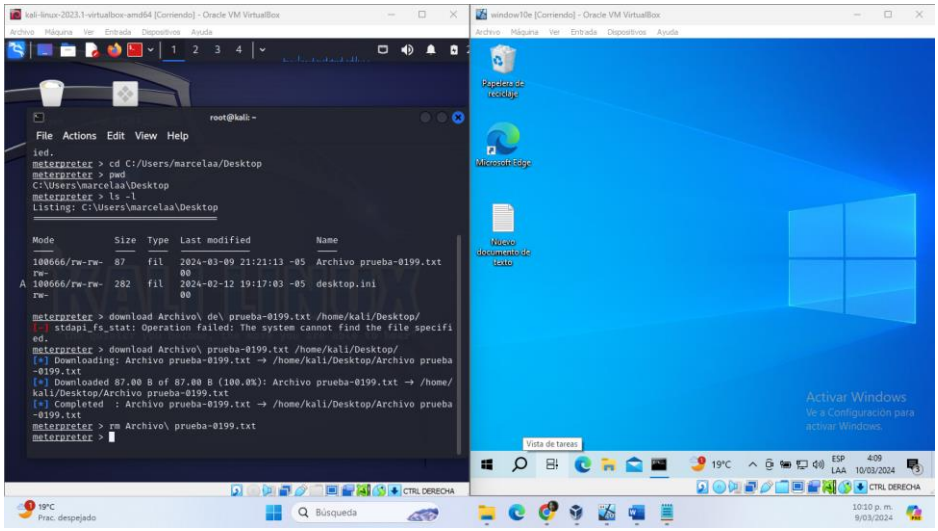
Los comandos de ejecución en Meterpreter no difieren significativamente de los utilizados en sistemas operativos Linux. La única diferencia radica en la interpretación de las rutas o ubicaciones de archivos, dado que la víctima utiliza un sistema operativo Windows.

Figura 16. Acceso desde Kali a máquina Windows



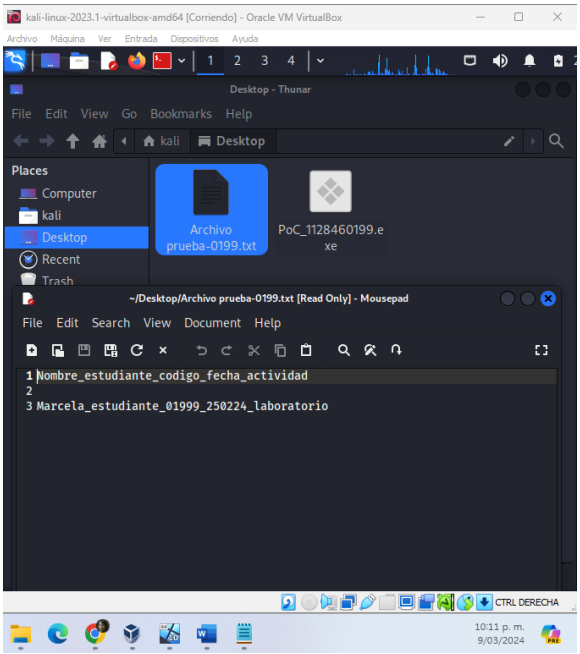
Fuente: El autor

Figura 17. Descarga y eliminación del archivo objetivo en la máquina Windows



Fuente: El autor

Figura 18. Demostración en la máquina atacante - documento objetivo



Fuente: El autor

2.4 ETAPA 4: ESTRATEGIAS DE DEFENSA & CONTENCIÓN DE ATAQUE INFORMATICO

En la cuarta y última fase, se pretende reforzar la protección de la infraestructura tecnológica de HackerHouse. Para ello, se implementarán estrategias de contención efectivas contra ataques cibernéticos originados por riesgos o vulnerabilidades en los activos de información.

2.4.1 RESPUESTA A LAS CIBERAMENAZAS: METODOLOGÍAS Y HERRAMIENTAS PARA LA IDENTIFICACIÓN Y CONTENCIÓN DEL ATAQUE (BANCO DE TRABAJO ETAPA #4)

La detección temprana y precisa de ataques de ciberseguridad y seguridad de la información es crucial para minimizar daños potenciales, como la pérdida de información confidencial, la interrupción de servicios, el daño reputacional e incluso las consecuencias legales y monetarias.

Este ejercicio se puede llevar a cabo mediante mecanismos de monitoreo, análisis, evaluación de seguridad y capacitación continua. Esto no solo fomenta un enfoque técnico, sino también proporciona el conocimiento necesario para actuar con pericia, rapidez y eficacia ante un ataque.

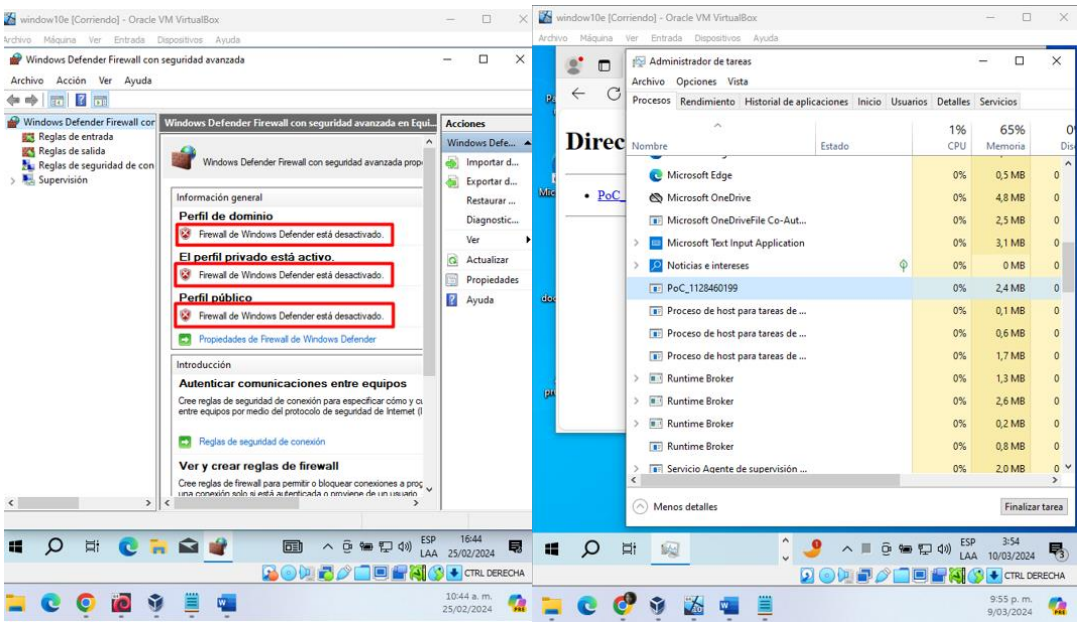
Es importante destacar que la identificación de amenazas no solo implica implementar estrategias de respuesta adecuadas para mitigar el daño, sino también establecer precedentes para prevenir incidentes futuros.

Durante la fase de investigación del incidente ocurrido en HackerHouse, se utilizó la metodología del Blue Team, que se divide en los siguientes pasos para analizar y contener el ataque:

- Monitoreo de la red
- Aislamiento de la red corporativa
- Recopilación de información
- Análisis de registros de red
- Conversación con el usuario afectado
- Detener el proceso o servicio desconocido
- Actualizar el estado de seguridad del componente
- Habilitar un programa de capacitación al área del recurso afectado o a la organización en general

Paso 1, Detección: Esta fase monitorea la red y el sistema en búsqueda de actividad inusual, lo que será de ayuda para reconocer el tipo de ataque que está afectando el componente. Por ejemplo ¿Existen lentitud inusual, bloqueos, nuevos procesos, incrementos de consumo en los registros, entre otros?

Figura 19. Análisis de procesos y configuraciones base – PC Windows



Fuente: El autor

Paso 2, Contención: Luego de detectar el ataque, se inicia la actividad para frenar su propagación en la red. Además, se implementan medidas correctivas a nivel de seguridad para prevenir futuros incidentes.

En el caso de la estación afectada, se puede desconectar las tarjetas de red para limitar el alcance del atacante. Posteriormente, es crucial activar las defensas locales de la estación, incluyendo el firewall, el antivirus (con protección en tiempo real, control de ejecución de aplicaciones y confirmación del usuario), y SmartScreen para el navegador.

Paso 3, Investigación: En esta fase, se llevan a cabo evaluaciones que permiten determinar la naturaleza del ataque y su objetivo. Es decir, se busca identificar el tipo de incidente ocurrido, su origen y el daño causado.

En el caso del banco de trabajo, durante la evaluación con el usuario afectado, se determinó que la falla tuvo su origen en un caso de ingeniería social. El atacante aprovechó las vulnerabilidades de la máquina Windows mediante inyección de código

Paso 4, Recuperación y mejora: En situaciones en las que existan procesos de respaldo de información, se inicia la activación del punto de restauración con el objetivo de eliminar el software malicioso del sistema. A continuación, se implementan medidas de endurecimiento en el dispositivo para corregir las vulnerabilidades que permitieron el ataque inicial. Estas acciones son esenciales para fortalecer la seguridad y prevenir futuros incidentes.

Paso 5, Documentación: Siguiendo los pasos previos, se genera el informe del incidente de seguridad. Además, se ha anexado una sección con recomendaciones y lecciones aprendidas para compartir con los interesados, con el objetivo de prevenir futuros incidentes de esta naturaleza.

2.4.2 ACCIONES DE HARDENIZACIÓN: HACKERHOUSE

El proceso de endurecimiento o hardenización es una actividad fundamental para la seguridad de los sistemas y salvaguardas de los activos de información frente a las amenazas digitales. Es decir, que corresponde a la actividad de habilitar y configurar medidas de seguridad que dificulten el acceso no autorizado, la explotación de vulnerabilidades y la ejecución de ataques[8].

[8] CALCOM. Windows 10 Hardening. (s.f). En línea. [19 marzo del 2024].; Disponible en: https://www.calcomsoftware.com/windows-10-solution-page/

La hardenización para HackerHouse incluye:

- **Reconfiguración de accesos y privilegios:** Deshabilitar el uso de privilegios administrativos locales en la máquina y configurar la política de escalamiento de privilegios para que solicite la contraseña de administrador con cambios de parámetros.

  Por otro lado, asignar accesos a la máquina en el dominio corporativo a través de grupos de seguridad para limitar los accesos no autorizados o de invitado en la estación de trabajo. También es importante establecer la política de contraseñas para preestablecer longitud, complejidad, historial y rotación.

- **Configuración de Red:** Segmentar la red corporativa en subredes o aislar el tráfico mediante VLANs para segregar el alcance por departamentos o redes de usuarios.

  Además, se debe habilitar una política para el proceso operativo y de mantenimiento de la red.

- **Configuración de Firewall:** Configurar reglas de tráfico para bloquear puertos, servicios y comunicaciones no requeridas o no autorizadas. Esto asegurará la comunicación específica únicamente entre dispositivos permitidos.

- **Configuración de servicios:** Por defecto, el sistema operativo Windows usa varios servicios que se ejecutan en segundo plano. Sin embargo, no todos ellos son necesarios para la funcionalidad del

sistema, por lo que se deben deshabilitar aquellos que no son imprescindibles.

- **Protección del sistema:** Establecer una política para los respaldos y la restauración de la información. Esto permitirá regresar a un estado anterior en caso de que ocurra un daño o una interrupción de los servicios.

- **Logs y monitoreo:** Configurar la captura y el almacenamiento de los logs del sistema, los usuarios y la red corporativa. Esta información será relevante para generar una auditoría forense en caso de problemas.

  Asimismo, establecer dentro de una línea base los parámetros de umbral de rendimiento para el monitoreo de la infraestructura. Esto apoyará la identificación de problemas de capacidad o de comportamiento inusual del activo.

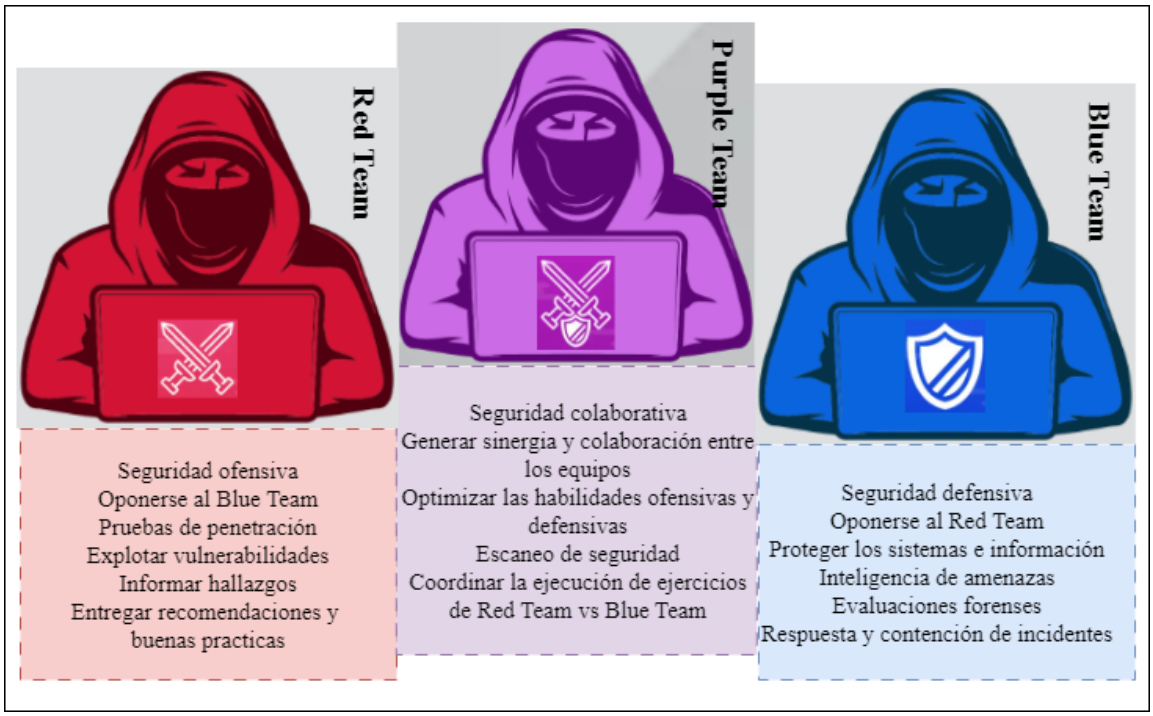
Cada una de estas acciones de endurecimiento de los componentes mitigara la materialización de futuros casos de aprovechamiento de vulnerabilidades, es decir que se reducirían los vectores de ataque conocidos sobre el sistema operativo Windows 10 y la infraestructura de la empresa HackerHouse.

2.4.3 DISTINCIÓN ENTRE LOS GRUPOS DE CIBERSEGURIDAD: EQUIPO PÚRPURA VS. EQUIPOS DE MANEJO DE INCIDENTES INFORMÁTICOS

En las pruebas de seguridad tradicionales, los equipos rojos y azules suelen trabajar de manera independiente. El equipo rojo simula a un atacante y ejecuta su plan sin conocimiento del equipo azul, que generalmente está compuesto por el equipo de seguridad de la organización. Sin embargo, la falta de comunicación entre ellos suele limitar la utilidad de las pruebas.

El propósito del equipo púrpura, una "combinación de rojo y azul", surge con la finalidad de optimizar la eficacia y la eficiencia de las evaluaciones de seguridad en los grupos involucrados. Entre sus características se incluye la retroalimentación y la colaboración entre todos durante la ejecución de las pruebas de seguridad, con el fin de brindar una cobertura integral desde la comprensión de la ofensiva y los mecanismos defensores. Esto trae consigo beneficios en la optimización del tiempo, los recursos y la cultura de aprendizaje continuo

Figura 20. Características de los Red, Purple y Blue Team



Fuente: El autor

Tabla 1. Diferencias entre el ejercicio de Red y Blue Team combinado con Purple Team

	ENFOQUE	OBJETIVO	RESPONSABILIDADES
BLUE TEAM	Proactivo/Reactivo	Defender la infraestructura	Implementar medidas de seguridad, monitorear la red, ejecutar pruebas defensivas y responder incidentes de seguridad
RED TEAM	Proactivo	Simular ataques en infraestructura, para hallar vulnerabilidades	Identificación y explotación de vulnerabilidades para informar al Blue Team

PURPLE TEAM	Proactivo/Reactivo	Optimizar la seguridad general de la organización	Coordinar ejercicios Red Team vs Blue Team, desarrollar estrategias de defensa y respuesta a incidentes y fomentar la cultura de seguridad
E. RESPUESTA A INCIDENTES	Reactivo	Responder a incidentes rápida y eficazmente	Investigar y contener incidentes de seguridad, para implementar el uso de buenas prácticas y mecanismos para reincidir en los fallos

Fuente: El autor

2.4.4 CIS "CENTRO PARA LA SEGURIDAD DE INTERNET": EN LA OPERACIÓN DE LOS EQUIPOS BLUE TEAM

Los controles de seguridad critica de CIS son un conjunto establecido y priorizado de buenas prácticas[9] en materia de Ciberseguridad analizadas y evaluadas para coincidir con los marcos de Ciberseguridad NIST, ISO, entre otros, con el propósito de que se usen en las organizaciones para fortalecer su postura frente a la Ciberseguridad de la infraestructura y los datos.

Dentro de los ejercicios de Red Team y Blue Team estos controles cumplen funciones como:

[9] CISECURITY; The 18 CIS Critical Security Controls; [Sitio web]; Desconocida; [Consulta: 21 marzo del 2024]; Disponible en: https://www.cisecurity.org/controls/cis-controls-list

- Establece marcos de referencia de seguridad que el equipo de Blue Team puede usar para evaluar su postura actual. Estos marcos ayudan a identificar vulnerabilidades o brechas, lo que permite priorizar las medidas de mitigación mediante las acciones o configuraciones sugeridas por CIS.

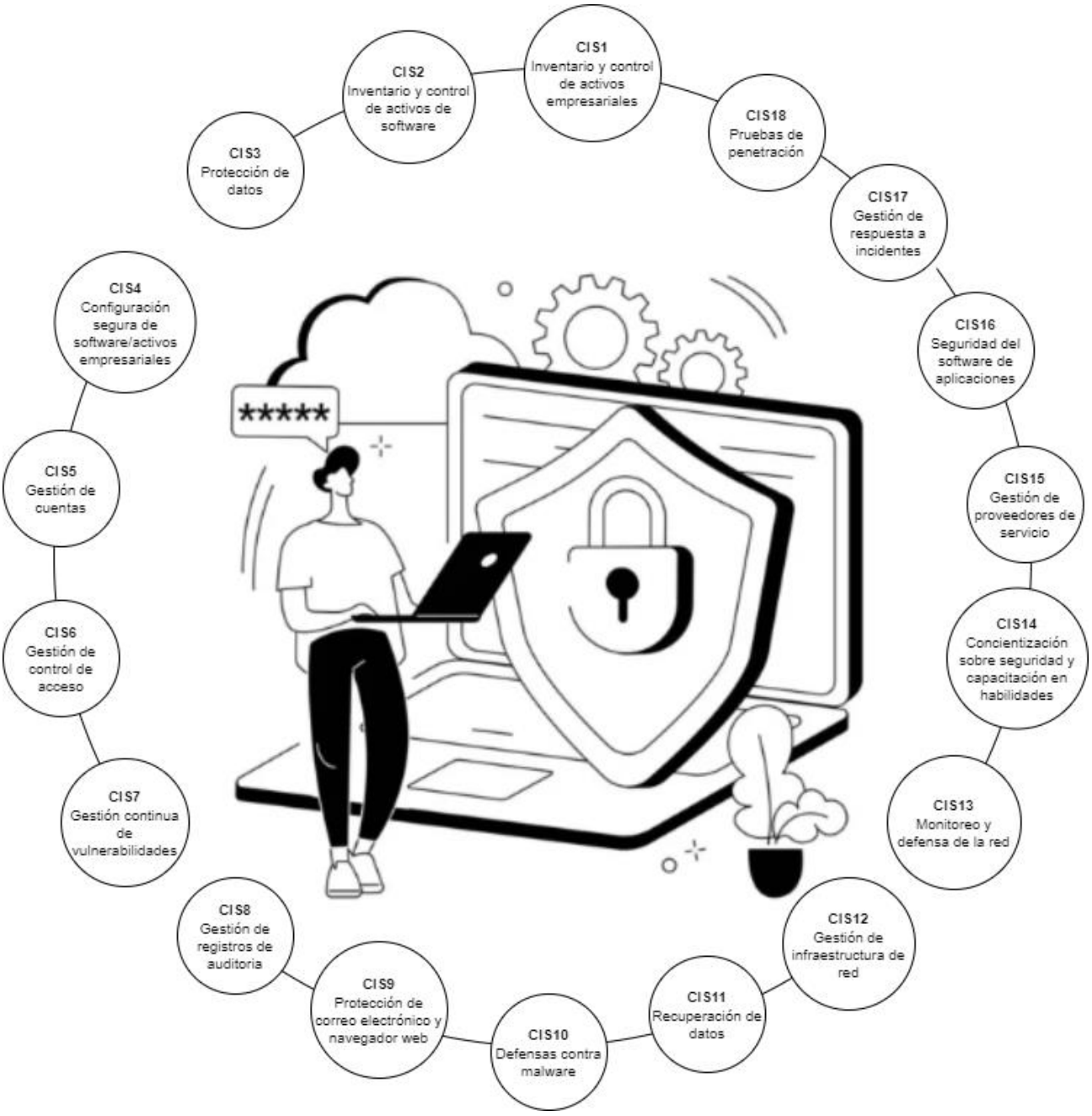
- Proporciona inteligencia de amenazas de forma actualizada, lo cual aporta al Blue Team en la comprensión de las amenazas y vulnerabilidades más recientes, lo que les permite corregir preventivamente sus estrategias de defensa.

- Proporciona formación en el ámbito de la ciberseguridad, lo cual estimula la comprensión de los conceptos y las mejores prácticas para abordar las tendencias de los delitos cibernéticos.

- Posee una comunidad amplia y activa a nivel mundial, a través de la cual los equipos de Blue Team pueden compartir y colaborar con otros profesionales conocimientos, experiencias y recomendaciones que les permitan fortalecer o resolver problemas de seguridad.

- Estos controles están alineados con diversos marcos regulatorios de seguridad, por lo que su implementación facilita el cumplimiento de las normas y regulaciones, lo que permite a los equipos de Blue Team evitar multas y sanciones.

Figura 21. Resumen controles CIS



Fuente: El autor

2.4.5 CARACTERISTICAS Y DIFERENCIAS: SIEM VS XDR

Las soluciones XDR y SIEM fueron diseñadas para optimizar la gestión de riesgos y/o amenazas en una organización. Para ello, reúnen y examinan información de seguridad en repositorios centralizados que les permiten mejor visibilidad y control de los datos, a continuación, se resumen sus principales características:

Tabla 2 SIEM VS XDR

Características	SIEM	XDR
Enfoque	Examinar y administrar registros centralizados	Recopilación de datos para mejorar la detección y respuesta de amenazas
Fuentes de datos	Registros de seguridad, eventos de red, datos de aplicaciones	Registros de seguridad, eventos de red, datos de endpoints, datos de la nube, datos de comportamiento de usuarios
Análisis	Correlación de eventos, búsqueda de patrones, generación de alertas	Análisis de comportamiento, machine learning, inteligencia de amenazas, correlación de múltiples fuentes
Respuesta	Investigación de incidentes, generación de informes, notificación a administradores	Aislamiento de amenazas, contención de ataques, automatización de respuestas
Casos de uso	Cumplimiento de normativas, auditoría de seguridad, gestión de riesgos	Detección de amenazas avanzadas, respuesta a incidentes, caza de amenazas

Escalabilidad	Adecuado para organizaciones de tamaño pequeño a mediano	Adecuado para organizaciones de tamaño mediano a grande
Complejidad	Menos complejo, basado en reglas y correlación	Más complejo, requiere experiencia en seguridad y análisis de datos
Costo	Menor costo de implementación y mantenimiento	Mayor costo de implementación y mantenimiento

Fuente: El autor

2.4.6 ANÁLISIS DE HERRAMIENTAS PARA DETECCIÓN DE ATAQUES INFORMATICOS: LICENCIA GPL

Las licencias públicas generales (GLP) son un tipo de permiso legal que se otorga al software libre. Este permiso brinda a los usuarios una amplia gama de facultades para su uso, modificación y distribución sin restricciones significativas. Por ello, una de sus principales fortalezas reside en la disponibilidad del código fuente para los usuarios, quienes pueden examinarlo a detalle para comprender su funcionamiento y adaptarlo según las necesidades de cada persona o empresa. Algunos ejemplos de estas herramientas son:

SNORT: Es una herramienta con capacidades para la detección de intrusiones (IDS) y prevención de intrusiones (IPS). Su modelo de operación se basa en la monitorización del tráfico y protocolos de red para detectar y prevenir diferentes tipos de ciberataques relacionados con vulnerabilidades de redes.

La herramienta tiene diferentes modos de operación, entre ellos:

Packet Sniffing: Captura y presenta de manera ordenada el flujo de información en la red.

Packet Logging: Registra y almacena el flujo de datos en la red en un archivo o log

Network Intrusion Detection: Examina los paquetes y los coteja con patrones preestablecidos para identificar comportamientos anómalos. Este es el modo de funcionamiento más relevante y popular de esta aplicación.

Por otro lado, su modelo de operación y mantenimiento de basa en tres reglas para detectar actividad maliciosa:

Reglas de comunidad: Disponible de forma abierta y gratuita para cualquier usuario, las reglas de uso son creadas y mantenidas por la comunidad de usuarios de Snort.

Reglas para usuarios registrados: Reglas personalizadas por proveedores del servicio, que tienen un costo de uso por ser específicas y abordar amenazas particulares según las necesidades del negocio.

Reglas para usuarios suscritos: Al igual que para los usuarios registrados, el uso de estas reglas tiene costo, no solo por la personalización de estas, sino también por el soporte y las actualizaciones de mantenimiento disponibles para los usuarios.

SECURITY ONION: Esta solución brinda herramientas para la detección de intrusos, el control de la seguridad de redes y el análisis de logs.

Entre sus principales beneficios se encuentra la combinación de herramientas de seguridad en su suite de servicios, su versatilidad le permite ser útil en una variedad de situaciones, como por ejemplo la suplantación de identidad, evaluación del comportamiento de la red y logs, entre otros.

OSSEC: Motor personalizable de recolección de eventos de seguridad basado en host, compatible con diversas plataformas como Linux, Solaris, AIX, BSD, Windows, macOS y VMware. Su función principal es analizar y supervisar registros, ejecutar comprobaciones y generar alertas en tiempo real para identificar patrones o comportamientos sospechosos que mitiguen el riesgo de un ataque o intrusión en los sistemas informáticos.

Este tipo de sistemas de detección de intrusiones se instala directamente en los dispositivos de los usuarios; por esta razón, monitorea las actividades de las estaciones y no de la red en general.

Tabla 3. Características OSSEC

VENTAJAS	DESVENTAJA
Bajo costo	Seguridad del código
Flexibilidad de personalización	Errores o falsos positivos por fallas de configuración
Alta compatibilidad	Alto consumo de capacidades físicas de infraestructura de TI
Facilidad en la gestión administrativa	Alta curva de aprendizaje

Fuente: El autor

SONATYPE: Herramienta para la administración de repositorios de código, que habilita la colaboración entre el desarrollo y el despliegue de software. Es decir, permite monitorizar un componente desde su desarrollo hasta su distribución para gestionar los riesgos y proteger la cadena de suministro del software.

Entre sus funcionalidades se encuentran: la identificación y corrección automática de debilidades en las dependencias de código abierto; la incorporación de herramientas de análisis de vulnerabilidades en los repositorios git ya existentes; y la prevención de ataques mediante la implementación de prácticas seguras de desarrollo a lo largo de los equipos de desarrollo y operaciones.

Tabla 4. Diferencias entre las herramientas GLP - Ciberseguridad

CARACTERISTICA	OSSEC	SONATYPE	SECURITY ONION	SNORT
PLATAFORMA	Multiplataforma	SaaS/Onpremise	On-premise	Multiplataforma
ENFOQUE	Detección de intrusos	Seguridad del desarrollo	Monitoreo y análisis de red	Análisis del tráfico de red
FLEXIBILIDAD	Configurable con varios entornos	Centrada para el Desarrollo de software	Adaptable a las necesidades	Habilita configuraciones especificas
SOPORTE	Comunidad y soporte comercial	Comunidad y soporte comercial	Comunidad y soporte comercial	Comunidad y soporte comercial

Fuente: El autor

3 APORTES DE LOS EQUIPOS DE SEGURIDAD EN LAS ORGANIZACIONES

Al conformar un equipo multidisciplinario que combine las características de los equipos de Blue Team, Red Team y Purple Team les permite a las organizaciones aportar de forma continua valor al negocio, ya que de forma preventiva siempre van a estar evolucionando y fortaleciendo sus mecanismos de defensa. Algunos de los beneficios consolidados de estos equipos en una empresa son:

Entrenamiento controlado y sinergia de los equipos: Simular ataques de seguridad y generar una comunicación transparente con todos los involucrados, las organizaciones tienen mayores oportunidades de conocer controladamente el impacto y los pasos de reacción que se deben tomar frente a un evento de seguridad. Además, al recibir retroalimentación constructiva de los diferentes involucrados desde diversas perspectivas, se fortalece la capacidad de respuesta.

Evaluaciones integrales: Con las evaluaciones de estos diferentes equipos, se permite identificar la capacidad real que pueden o no tener las organizaciones para proteger sus activos de información críticos, entre los cuales destacan no solo los relacionados con lo tecnológico, sino también sus procesos y personal.

Mejora continua: Identificar tempranamente y de forma controlada fallos y vulnerabilidades, se puede verificar la efectividad de las medidas de seguridad actuales con el propósito de ajustarlas a las demandas actuales. Es decir,

facilita la toma de decisiones frente a los cambios en procesos, políticas y controles para una mejor reacción en casos reales.

Eficiencia de los procesos: Al considerar la combinación de la seguridad ofensiva y defensiva, no solo se facilita la integración y comunicación de los diferentes equipos, sino también fortalece las herramientas y mecanismos organizacionales para tener defensas sólidas e integrales.

4 POLÍTICAS DE SEGURIDAD Y BUENAS PRACTICAS PARA TI

El uso de políticas de seguridad y buenas prácticas en las tecnologías de la información es un mecanismo para garantizar la protección, integridad y disponibilidad de los datos y sistemas en las organizaciones. Es decir, agilizan un ambiente eficaz e íntegro a través del cual la constante sea la seguridad de los activos de información. A continuación, se detallan algunas recomendaciones para el escenario expuesto en el banco de trabajo del seminario:

Política de control de acceso: Establece los requisitos (reglas de negocio) para otorgar roles y permisos dentro de la infraestructura de TI.

- Define roles y permisos para usuarios funcionales y administradores
- Define controles de ciberseguridad como MFA para aumentar la seguridad en la red corporativa
- Modifica o revoca los accesos cuando existen novedades

Política de contraseñas: Establece los controles y/o requisitos que se deben cumplir dentro de la organización para fomentar el uso de contraseñas fuertes y rotativas.

- Exige la complejidad que deben tener las contraseñas de acceso
- Exige el cambio periódico de las contraseñas

Política copias de seguridad: Establece el procedimiento y recurrencia mínima de los respaldos de los datos críticos de la organización.

- Automatiza la captura de respaldos de información
- Define la custodia y rotación de las copias de seguridad
- Establece procesos de auditoria para las restauraciones de información

Política de gestión de dispositivos: Establece los controles de seguridad que deben cumplir mínimamente los dispositivos conectados a la red.

- Habilita soluciones para la administración de dispositivos (PC, móviles, discos, entre otros)
- Controla el uso de dispositivos personales en la red corporativa
- Define los privilegios en los dispositivos corporativos

Política de auditoría y monitoreo: Define los controles para vigilar y evaluar procesos, usuarios e infraestructura.

- Configura herramientas para el monitoreo de la red y el almacenamiento de registros

- Define los controles para la actualización y supervisión de los activos de información
- Define la periodicidad de auditorías y evaluaciones internas o externas

Política de actualizaciones y parches: Establece los controles y la cobertura mínima que se debe cumplir por parte de los administradores y responsables de TI en los activos de información para mantener los sistemas y aplicaciones actualizadas.

- Ejecuta evaluaciones o escaneos periódicos de vulnerabilidades
- Gestiona la aplicación de parches de seguridad correctivos

Política para gestión de incidentes: Establece un marco de acción para responder a eventos que puedan afectar la seguridad de la información y los sistemas de la empresa. Minimizando el impacto negativo de estos incidentes y garantizar la continuidad del negocio

- Crear un equipo de respuesta a incidentes
- Define la guía para el manejo de incidentes
- Ejecuta simulacros periódicos para evaluar la seguridad de los sistemas y el manejo de las situaciones por los responsables

Política de Educación y Concienciación: Esta política se centra en educar y concientizar a los empleados sobre la importancia de la seguridad de la información y los riesgos asociados al manejo inadecuado de la misma

- Genera programas de capacitaciones recurrentes

- Difunde información relacionada con temas de seguridad de la información y ciberseguridad
- Fomenta el cumplimiento normativo en la organización

5 CONCLUSIONES

- Durante mi análisis del acuerdo de confidencialidad, identifiqué diversas anomalías en el documento. Estas irregularidades sugieren que el acuerdo implementado para la contratación de personal contraviene la ley colombiana que supervisa la actividad laboral de la compañía en el ámbito profesional. Además, se incumplen normas éticas de la profesión, como la obligación de guardar silencio sobre actividades ilícitas, la limitación del derecho a la defensa y la responsabilización del empleado por información ilegal en nombre de la empresa. Estas acciones afectan tanto la integridad personal como profesional. Es crucial abordar estas preocupaciones para garantizar un ambiente laboral ético y legalmente sólido.

- Se documenta la metodología y el proceso de auditoría ejecutado para el caso expuesto en el Anexo 4. En este proceso, se lograron identificar vulnerabilidades tanto técnicas como a nivel de personal, las cuales permitieron la materialización de un incidente de seguridad que comprometió información interna de la organización. Es decir, se concluye que no solo las malas prácticas de seguridad influyeron en el caso, sino que también la responsabilidad y el accionar del responsable de la máquina desempeñaron un papel fundamental en la materialización del hecho. Es crucial abordar estas vulnerabilidades y mejorar tanto las prácticas de seguridad como la capacitación del personal para prevenir futuros incidentes similares.

- En la contención del ataque de ciberseguridad, se identificó que el ataque presentado fue una mezcla de vectores de ataque que incluyeron inyección de código, malware activado por el usuario responsable de la máquina e ingeniería social. Estos factores desencadenaron la elevación de privilegios y el robo de información. La afectación a la empresa HackerHouse podría resultar no solo en la pérdida de información, sino también en la reputación dañada y medidas punitivas impuestas por las autoridades de supervisión y regulación debido a las fallas en los mecanismos de defensa y la posible afectación de usuarios internos y externos a la organización.

  Por otro lado, durante la evaluación del Red Team, se identificó que en el problema y en la conversación con el usuario no se hace mención sobre controles o procedimientos para el manejo y respaldo de la información. Esta omisión afecta la recuperación del sistema por completo, ya que no se tiene un punto de retorno de la máquina Windows. Por lo tanto, dentro de las recomendaciones y lecciones aprendidas, se sugiere implementar este procedimiento como una de las buenas prácticas y mejoras a los controles actuales. Es fundamental establecer políticas y procedimientos sólidos para asegurar la protección y la integridad de los activos corporativos.

6 RECOMENDACIONES

Para fortalecer la postura de seguridad en HackerHouse a raíz del incidente de seguridad presentado, es necesario implementar estrategias de respuesta efectivas frente a las amenazas y vulnerabilidades que afectan los activos de información

A continuación, se detallan algunas buenas prácticas y mecanismos que reforzarían la seguridad en la infraestructura y red informática de la empresa:

- Los responsables de Ciberseguridad deberán implementar medidas de seguridad para la gestión de identidades y accesos, como por ejemplo uso de MFA, habilitación del mínimo privilegio y uso de auditorías para los usuarios en la red corporativa. Estas acciones reducirían el aprovechamiento del uso indebido de privilegios y la fuga de información.

- Implementar el control de riesgos, donde se incluya el protocolo de respuesta para eventos inesperados y revisiones internas/externas de forma periódica para analizar la protección de la infraestructura TI.

- Implementar y mantener el uso de herramientas de seguridad perimetral o EndPoints para la protección a nivel web y local desde la detección y bloqueo de actividades sospechosas. Así mismo se debe establecer un sistema de control de aplicaciones para evitar la ejecución de software no autorizado.

- Los responsables de Ciberseguridad deberán construir "El manual de políticas de seguridad y buenas prácticas" donde se debe contemplar las medidas para controlar los privilegios de administración de los equipos informáticos para restringir la instalación de software o cualquier otro componente y el uso de sitios web no corporativos.

- Implementar planes de formación para los empleados de la empresa es fundamental para fortalecer la posición de seguridad informática. Esto es especialmente relevante dado que existen numerosos ataques cibernéticos que se aprovechan de la falta de conocimiento y la desinformación.

- Establecer e implementar procedimientos y protocolos vinculados al seguimiento, control y actualización de las herramientas de detección e identificación de vulnerabilidades para una gestión adecuada.

7 BIBLIOGRAFÍA

AGUILAR, Mauricio; Principales herramientas de seguridad de código abierto; [Sitio web]; Desconocida; [Consulta: 20 marzo del 2024]; Disponible en: https://blog.udpsa.com/principales-herramientas-de-seguridad-de-codigo-abierto/

ARIAS, D; Proporcionalidad, pena y principio de legalidad; [Sitio web]; Barranquilla: UDA; [Consulta: 18 febrero del 2024]; Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972012000200005#:~:text=El%20art%C3%ADculo%203%20del%20CP,de%20necesidad%2C%20proporcionalidad%20y%20razonabilidad.

CALCOM; Windows 10 Hardening; [Sitio web]; Desconocida; [Consulta: 19 marzo del 2024]; Disponible en: https://www.calcomsoftware.com/windows-10-solution-page/

CAPARROSO, J; Ataques a EPM y Sanitas encienden las alarmas sobre la ciberseguridad en Colombia; [Sitio web]; Bogotá, Colombia; [Consulta: 20 febrero del 2024]; Disponible en: https://forbes.co/2023/01/25/tecnologia/ataques-a-epm-y-sanitas-encienden-las-alarmas-sobre-la-ciberseguridad-en-colombia

CCIT; IA Para la protección y prevención de amenazas; [Sitio web]; Desconocida; [Consulta: 19 marzo del 2024]; Disponible en: https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

CHECK POINT; ¿What is a Purple Team?; [Sitio web]; Norteamérica; [Consulta: 19 marzo del 2024]; Disponible en: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-purple-team/

CHECK POINT; XDR frente a SIEM; [Sitio web]; Norteamérica; [Consulta: 19 marzo del 2024]; Disponible en: https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-xdr-extended-detection-and-response/xdr-vs-siem/

CISECURITY; The 18 CIS Critical Security Controls; [Sitio web]; Desconocida; [Consulta: 21 marzo del 2024]; Disponible en: https://www.cisecurity.org/controls/cis-controls-list

CONGRESO DE LA REPÚBLICA; Ley 906 Por la cual se expide el Código de Procedimiento Penal; [Sitio web]; Bogotá, Colombia; [Consulta: 18 febrero del 2024]; Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_09060_204a_pr001.html#67

CORTE CONSTITUCIONAL; Acción de tutela contra providencias judiciales-Reiteración de jurisprudencia sobre procedencia excepcional; [Sitio web]; Bogotá, Colombia; [Consulta: 18 febrero del 2024]; Disponible en: https://www.corteconstitucional.gov.co/relatoria/2017/t-018-17.htm

CORTES, Sandra; Capacidades Técnicas, Legales Y De Gestión Para Equipos Blue team Y Red team; [Sitio web]; Chiquinquirá: UNAD; [Consulta: 25 febrero del 2024]; Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/50306/secortesc.pdf?sequence=1&isAllowed=y

FASTLY; Sonatype; [Sitio web]; Fulton: MD; [Consulta: 20 marzo del 2024]; Disponible en: https://www.fastly.com/es/customers/sonatype/

FORTRA; ¿Qué es el pentesting?; [Sitio web]; Desconocida; [Consulta: 25 febrero del 2024]; Disponible en: https://www.fortra.com/es/soluciones/ciberseguridad/pentesting

FUNCION PUBLICA; Ley 1708 de 2014; [Sitio web]; Bogotá, Colombia; [Consulta: 17 febrero del 2024]; Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=56475

GARCIA, Víctor; Security Onion: qué es y cómo funciona; [Sitio web]; Venezuela; [Consulta: 19 marzo del 2024]; Disponible en: https://www.serviciosvartech.com/security-onion-que-es-y-como-funciona/#:~:text=Security%20Onion%20funciona%20como%20un,comportamiento%20sospechosos%20y%20detectar%20amenazas

GIRALDO, Luisa; Ataque cibernético a Colsanitas: detrás estaría organización criminal de talla internacional; [Sitio web]; Bogotá, Colombia; [Consulta: 20 febrero del 2024]; Disponible en: https://canal1.com.co/noticias/ataque-

cibernetico-a-colsanitas-detras-estaria-organizacion-criminal-de-talla-internacional/

GOMEZ, José; Test De Penetracion Pentesting Aplicado En La Empresa Megaseguridad Para Evaluar Vulnerabilidades Y Fallas En El Sistema De Información; [Sitio web]; Bogotá: UNAD; [Consulta: 26 febrero del 2024]; Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/42327/Jlgomezv.pdf?sequence=3&isAllowed=y

ITECHSAS; Que se sabe del ciberataque a Keralty EPS Sanitas y Colsanitas; [Sitio web]; Desconocida; [Consulta: 20 febrero del 2024]; Disponible en: https://www.itechsas.com/blog/recursos/que-se-sabe-del-ciberataque-a-keralty-eps-sanitas-y-colsanitas/

KAUFER; Ian. Human Exploits in Cybersecurity: A Social Engineering Study; [Sitio web]; Arizona; [Consulta: 28 febrero del 2024]; Disponible en: https://eller.arizona.edu/sites/default/files/ian_kaufer_sfs_masters_paper.pdf

KEEPCODING. ¿Qué es OSSEC?; [Sitio web]; Ucrania; [Consulta: 19 marzo del 2024]; Disponible en: https://keepcoding.io/blog/que-es-ossec/

KEEPCODING. ¿Qué es Snort en ciberseguridad?; [Sitio web]; Ucrania; [Consulta: 19 marzo del 2024]; Disponible en: https://keepcoding.io/blog/que-es-snort-en-ciberseguridad/

LEYES; Código de Procedimiento Penal. Artículo 309; [Sitio web]; Bogotá, Colombia; [Consulta: 17 febrero del 2024]; Disponible en: https://leyes.co/codigo_de_procedimiento_penal/309.htm

LOPEZ, Miguel; Análisis forense digital; [Sitio web]; Desconocida; [Consulta: 28 febrero del 2024]; Disponible en: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

MANAGEENGINE; ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)?; [Sitio web]; Ontario, Canadá; [Consulta: 20 marzo del 2024]; Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

MINTIC; En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia; [Sitio web]; Bogotá, Colombia; [Consulta: 20 febrero del 2024]; Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

MINTIC; LEY 1712 DE 2014; [Sitio web]; Bogotá, Colombia; [Consulta: 17 febrero del 2024].; Disponible en: https://www.mincit.gov.co/ministerio/normograma-sig/evaluacion-y-seguimiento/leyes/ley-1712-de-2014.aspx#:~:text=ART%C3%8DCULO%204o.&text=En%20ejercicio%20del%20derecho%20fundamental,solamente%20podr%C3%A1%20ser%20restringido%20excepcionalmente

OLANO, German; ¿Qué es Ransomhouse?; [Sitio web]; Valparaíso, Antioquia; [Consulta: 20 febrero del 2024].; Disponible en: https://es.linkedin.com/pulse/qu%C3%A9-es-ransomhouse-germ%C3%A1n-andr%C3%A9s-olano-trejos

PENAGOS, Cristian; Análisis De Metodologías De Ethical Hacking Para La Detección De Vulnerabilidades En Las Pymes; [Sitio web]; Medellín: UNAD; [Consulta: 26 febrero del 2024]; Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30302/ccpenagosm.pdf?sequence=1&isAllowed=y

POLICIA; Ley 1273 de 2009; [Sitio web]; Bogotá, Colombia; [Consulta: 17 febrero del 2024]; Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos#:~:text=Art%C3%ADculo%20269A%3A%20Acceso%20abusivo%20a,el%20leg%C3%ADtimo%20derecho%20a%20excluirlo

RAIGOSO, Luis; SIEM vs SOAR vs XDR: ¿Cuáles son las diferencias y cuál es el adecuado para tu organización?; [Sitio web]; Boyacá, Colombia; [Consulta: 19 marzo del 2024]; Disponible en: https://es.linkedin.com/pulse/siem-vs-soar-xdr-cu%C3%A1les-son-las-diferencias-y-cu%C3%A1l-es-luis-jos%C3%A9

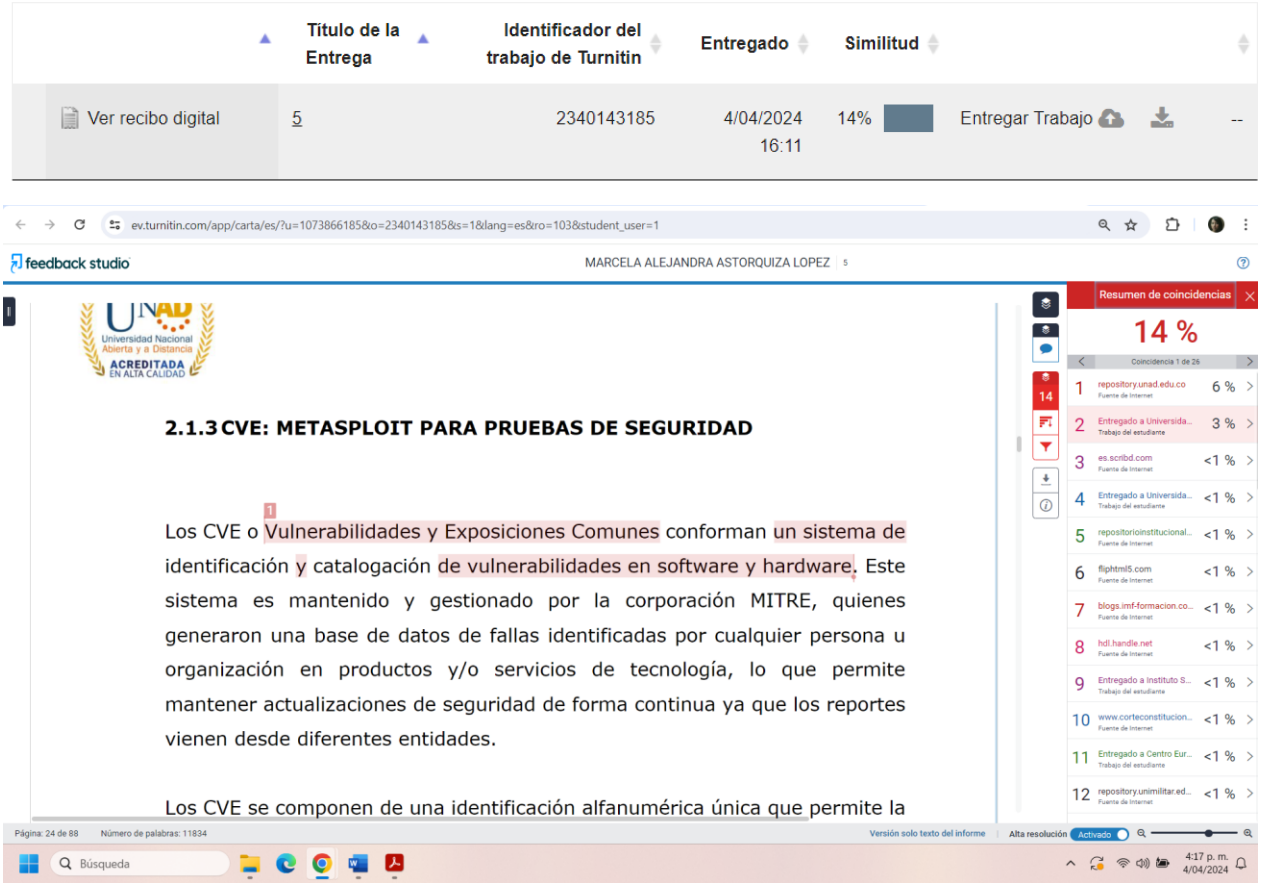
SIC; Ley 1273 del 2009; [Sitio web]; Bogotá, Colombia; [Consulta: 17 febrero del 2024]; Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

UREÑA, Jairo; 7.5 - Payloads & Msfvenom - Curso Introducción al Hacking & Pentesting; [Sitio web]; Republica dominicana; [Consulta: 25 febrero del 2024]; Disponible en: https://www.youtube.com/watch?v=fzBaUXpWsk4

WANG.Z, ZHU. H, LIMIN.S; Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods; [Sitio web]; Beijín, China; [Consulta: 29 febrero del 2024]; Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9323026

ANEXOS

Anexo A. Evidencia de revisión de plagio: Turnitin



	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud		
Ver recibo digital	5	2340143185	4/04/2024 16:11	14%	Entregar Trabajo	--

Fuente: El autor

Anexo B.. Enlace de sustentación

Youtube: https://youtu.be/sBgsoE3G40M