Capacidades técnicas, legales y de gestión para equipos blue team y red team

Kelly Patricia Maturana Rentería

Asesor

Luis Fernando Zambrano Hernández

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Con profundo amor y gratitud, dedico este trabajo en primer lugar a Dios, por permitirme avanzar en este camino del conocimiento y brindarme la fortaleza necesaria para seguir adelante, pues sin Él nada sería posible. Agradezco de corazón a mis padres y a toda mi familia, quienes con su ejemplo y enseñanzas han formado en mí los valores que me impulsan a superarme cada día. A mi pareja, por estar a mi lado en los momentos más exigentes, por sus palabras de ánimo y su constante apoyo que han sido fundamentales para continuar con mis responsabilidades. Y a mis hermanos, por estar presentes siempre que los he necesitado, ofreciéndome su respaldo incondicional.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas aquellas personas que, de una u otra manera, contribuyeron y acompañaron este proceso formativo. En primer lugar, a la Universidad Nacional Abierta y a Distancia (UNAD), por ofrecer un modelo educativo flexible y accesible, que permite a quienes, como yo, deben equilibrar sus estudios con responsabilidades laborales y personales, avanzar en su formación profesional sin barreras.

También extiendo mi gratitud a los tutores, quienes con dedicación, paciencia y compromiso académico estuvieron dispuestos a guiar, aclarar dudas y aportar sus conocimientos para nuestro crecimiento. Su acompañamiento fue clave para consolidar el aprendizaje a lo largo de esta etapa.

Y por supuesto, a mis compañeros de estudio, con quienes compartí este camino. Aunque en algunos casos la interacción fue breve, cada colaboración, consejo o intercambio de ideas aportó significativamente al cumplimiento de este objetivo. Gracias por ser parte de esta experiencia y por sumar al desarrollo de este logro colectivo e individual.

Resumen

En la búsqueda de dar soluciones a los problemas presentado, surge la necesidad de investigar y lograr el análisis de alguna técnica y/o herramienta que permitan mitigar riesgos e identificar vulnerabilidades que pongan en peligro la seguridad y permanencia de las empresas en el mercado.

La evolución del internet y las redes informáticas ha generado avances tecnológicos significativos, pero también ha incrementado los riesgos cibernéticos, especialmente en el ámbito empresarial. La necesidad de proteger datos críticos frente a individuos maliciosos ha impulsado el desarrollo de estrategias y herramientas como Red Team y Blue Team, que trabajan de manera complementaria para fortalecer la seguridad informática.

El Red Team simula ataques reales para identificar vulnerabilidades, mientras que el Blue Team responde implementando medidas defensivas para mitigarlas. Este enfoque permite a las organizaciones analizar y reforzar sus sistemas, garantizando la confidencialidad, integridad y disponibilidad de la información. A través de pruebas controladas, se logra proteger los activos digitales, minimizar riesgos y fortalecer la confianza en las operaciones empresariales frente a un entorno cibernético en constante cambio.

Palabras claves: Red Team, Blue Team, vulnerabilidades, seguridad informática

Abstract

In the search for solutions to the problems presented, there is a need to research and analyze techniques and/or tools that mitigate risks and identify vulnerabilities that jeopardize the security and permanence of companies in the market.

The evolution of the internet and computer networks has generated significant technological advances, but it has also increased cyber risks, especially in the business world. The need to protect critical data from malicious actors has driven the development of strategies and tools such as Red Team and Blue Team, which work together to strengthen cybersecurity.

The Red Team simulates real attacks to identify vulnerabilities, while the Blue Team responds by implementing defensive measures to mitigate them. This approach allows organizations to analyze and strengthen their systems, ensuring the confidentiality, integrity, and availability of information. Through controlled testing, digital assets are protected, risks are minimized, and confidence in business operations is strengthened in the face of a constantly changing cyber environment.

Keywords: Red Team, Blue Team, vulnerabilities, computer security

Tabla de Contenido

Lista de Figuras

Glosario

Amenaza: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad. (www.incibe.es, 2021)

Blue team: Término empleado en ciberseguridad (proveniente del ámbito militar) para designar un equipo humano encargado de detener ataques de intrusión en redes y sistemas del ámbito corporativo por parte de atacantes reales. Su misión es corregir las vulnerabilidades o deficiencias detectadas por un equipo rojo, el cual realiza simulaciones de ataques controlados, así como detener posibles ataques reales. Este tipo de equipos están exclusivamente especializados en monitorizar y reforzar la seguridad de la empresa. (incibe, 2021, pág. 41)

Ciberseguridad: La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales.

Delincuencia informática: Los delitos informáticos, son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores.

Feedback: es utilizado, por ejemplo, para evaluar a una persona, una empresa, un producto o un servicio. Por lo tanto, el feedback consiste en una forma de diagnóstico que permite identificar puntos positivos y puntos negativos de aquello que está siendo evaluado.

Hackear: Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados. (incibe, 2021, pág. 47)

Licencias: es una autorización que otorga un autor o autores que permiten el derecho a terceras personas de utilizar su creación o recurso.

Pentesting: Una prueba de penetración, o pentest, es una prueba de seguridad que lanza un ciberataque simulado para encontrar vulnerabilidades en un sistema informático. (ibm, 2025)

Red team: Término empleado en ciberseguridad, para designar un equipo humano encargado de realizar pruebas de intrusión en redes y sistemas del ámbito corporativo con el fin de evaluar la ciberseguridad de la empresa y detectar vulnerabilidades. Se trata en realidad de una simulación de ataques controlados sin causar daño, en el que las deficiencias detectadas se reportan al equipo azul, encargado de subsanarlas. (incibe, 2021, pág. 41)

Redes informáticas: Se entiende por redes informáticas, redes de comunicaciones de datos o redes de computadoras a un número de sistemas informáticos conectados entre sí mediante una serie de dispositivos alámbricos o inalámbricos, gracias a los cuales pueden compartir información.

Seguridad defensiva: hace referencia a un grupo de profesionales los cuales se enfocan en la protección de los activos de una organización ante cualquier tipo de amenaza.

Seguridad informática: La seguridad informática es el conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado.

Seguridad ofensiva: conjunto de herramientas o soluciones que tienen como objetivo identificar en tiempo real el grado de exposición que tiene una organización y cómo afectaría en cualquier incidente que se produjera.

TTPs: protocolo utilizado para enviar datos entre un navegador web y un sitio web.

Vulnerabilidades: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto. (incibe, 2021, pág. 77)

Introducción

Los ataques informáticos han evolucionado, haciendo cada vez más complejo controlar las amenazas en el mundo digital. Las empresas, preocupadas por la seguridad de sus sistemas, deben contar con equipos capacitados para mitigar riesgos y proteger sus datos.

En este contexto, las herramientas Red Team y Blue Team se presentan como estrategias clave para analizar vulnerabilidades y fortalecer la seguridad. Estas prácticas, realizadas en tiempo real y bajo condiciones controladas, permiten identificar fallos en la red y los sistemas de información, ofreciendo soluciones para reducir riesgos. Su implementación adecuada garantiza resultados positivos en la protección de los activos empresariales.

Objetivos

Objetivo General

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI, analizando y aplicando leyes dirigidas a la seguridad informática, asegurando así el cumplimiento ético de las acciones realizadas.

Objetivo Especifico

analizar las leyes y normas por las cuales se rige la seguridad informática, con el fin de conocer la normatividad en ciberseguridad y protección de datos para asegurar que las pruebas y estrategias cumplan los requisitos, y de esta manera mitigar riesgos legales.

Conocer algunas estrategias implementadas por los equipos red team y blue team en la búsqueda de vulnerabilidades a través de pruebas controladas dentro de un sistema, para su previa protección y mitigación de riesgos.

Proponer estrategias de contención y mitigación efectiva, las cuales logren reducir en gran medida riesgos cibernéticos, y fortalezcan la infraestructura tecnológica.

Desarrollo del informe

1. Aspectos que aporten al desarrollo de estrategias de RedTeam &BlueTeam

Dentro de los apartes tenidos en cuenta para el desarrollo de esta actividad, se tuvieran en cuenta los siguientes:

1.1.Leyes colombianas sobre delitos informáticos.

Dentro del margen legal en Colombia los delitos informáticos se encuentran, la protección de datos personales es regulados por algunas normas y leyes las cuales brindan directrices para proteger la integridad de personas, la protección de informacion y demás. Entre estas normas encontramos la.

- La **Ley 1273 de 2009**: esta es una ley penal, la cual contiene informacion para la protección de la información y de datos. todo delito informático ocurrido, que violente o vulnere la integridad de personas o casas, es castigado por medio de esta ley. El acceso indebido a un sistema, daños a sistemas informáticos o la suplantación de sitios web son delitos informáticos castigados con esta ley.
- La **Ley 1581 de 2012**: esta ley Protege los Datos Personales, estableciendo normas de como salvaguardar, y utilizar los datos personales de una persona. El derecho a la privacidad de los datos personales y el tratamiento de datos, son algunas de las características las cuales se acogen en esta ley.
- **Decreto 1377 de 2013:** este decreto va de la mano de la ley 1581, puesto que por medio de este fue Reglamentada la Ley 1581 de 2012, la cual dispone la protección de datos personales.

- Esta **Ley 1928 de 2018** se estableció a través de un convenio, el cual acoge los Ciberdelitos Internacionales, es decir por medio de esta ley se establece la colaboración internacional ante delitos de fraude informático internacional, como lo puede ser el tráfico de contenido infantil en la web.

1.2.Etapas para la realización de pruebas de penetración o pentesting.

Las pruebas de pentesting, juegan un papel muy importante en el mundo de la ciberseguridad, debido a que estas, por medio de la exploración permiten identificar de manera controlada las posibles vulnerabilidades que existen en un sistema informático. Para la realización de pruebas de penetración es necesario seguir una secuencia de pasos o cumplir con diferentes etapas para lograr con éxito el ataque. Como lo son.

- Etapa de reconocimiento
- Etapa de escaneo
- Etapa de explotación
- Etapa de post – explotación
- Fase de reporte

1.3. Herramientas importantes en la realización de pentestinhg.

Metasploit: Es un marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema. Podríamos decir que metasploit es un marco muy versátil, el cual proporciona herramientas de explotación y post explotación, donde su papel fundamental son las pruebas de penetración, con el fin de detectar y solucionar los fallos antes de que sean explotados por un atacante. (Ciberseguridad.com, 2021)

Nmap: (“mapeado de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.

En otras palabras, Nmap, es una herramienta esencial para la exploración y análisis de una red, puesto que esta permite identificar actividades ejecutadas en nuestro sistema, como lo es. La detección de puertos abiertos, sistema operativo, servicios en entre otras características, y por ende permite identificar vulnerabilidades existentes en la red.

OpenVas: Es un escáner de vulnerabilidades de código abierto multiplataforma que cuenta con una aplicación web que nos permite realizar búsquedas de vulnerabilidades en uno o varios equipos dentro de una red. OpenVAS clasifica estas vulnerabilidades en tres categorías. Alto riesgo, medio riesgo y bajo riesgo.

En síntesis, OpenVas es una herramienta importante y esencial para evaluar las vulnerabilidades existentes en un sistema y en las redes, debido a su capacidad de identificar y reportar estas vulnerabilidades. lo que permite fortalecer la defensa e infraestructura de la red.

Servicios en línea

ExploitDB: es una aplicación web que reúne bases de datos públicas con exploits para vulnerabilidades conocidas, en lo que contribuyen los usuarios. Dichos exploits pueden ser consultados, descargados y utilizados por pentesters de todo el mundo de forma gratuita para mejorar la calidad de sus auditorías de ciberseguridad.

CVE: Es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware que está desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad. CVE proporciona una base de datos de referencia que permite a los investigadores de seguridad, fabricantes y responsables de seguridad de las organizaciones identificar y gestionar de manera más eficiente los problemas de seguridad.

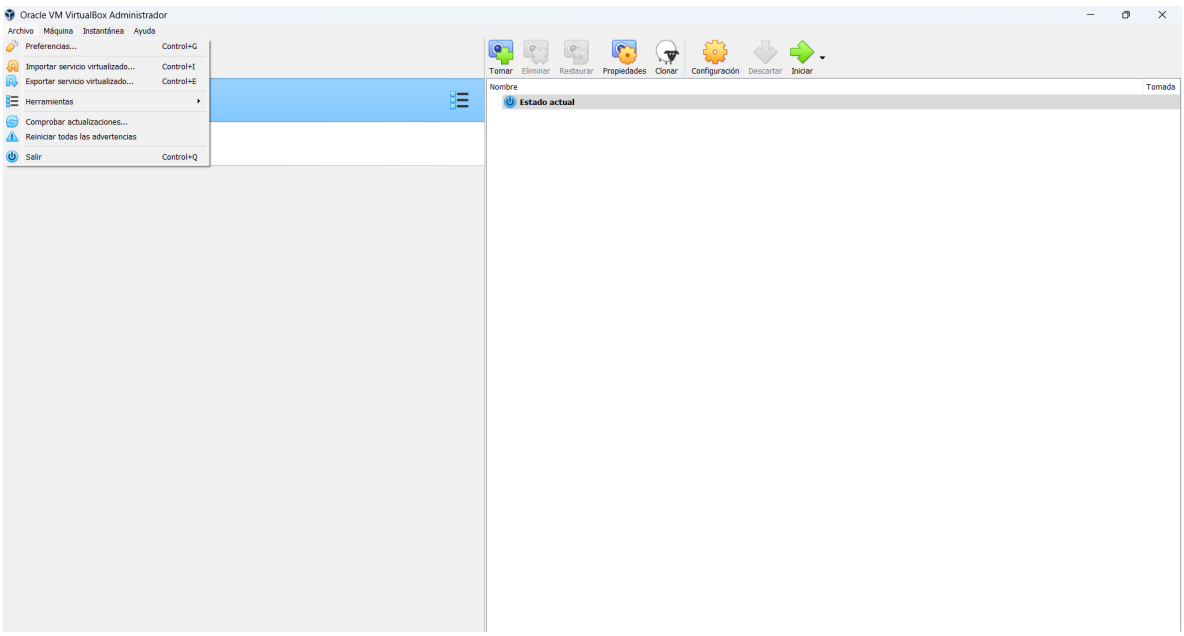
1.4.configuración del banco de trabajo

Para la realización de esta actividad, fue necesario el uso de una máquina virtual. Para este caso se descargó la herramienta virtual box. Y luego realizar la instalación de la maquina Kali Linux y Windows.

Máquina virtual “VirtualBox” en su última versión.

Figura 1

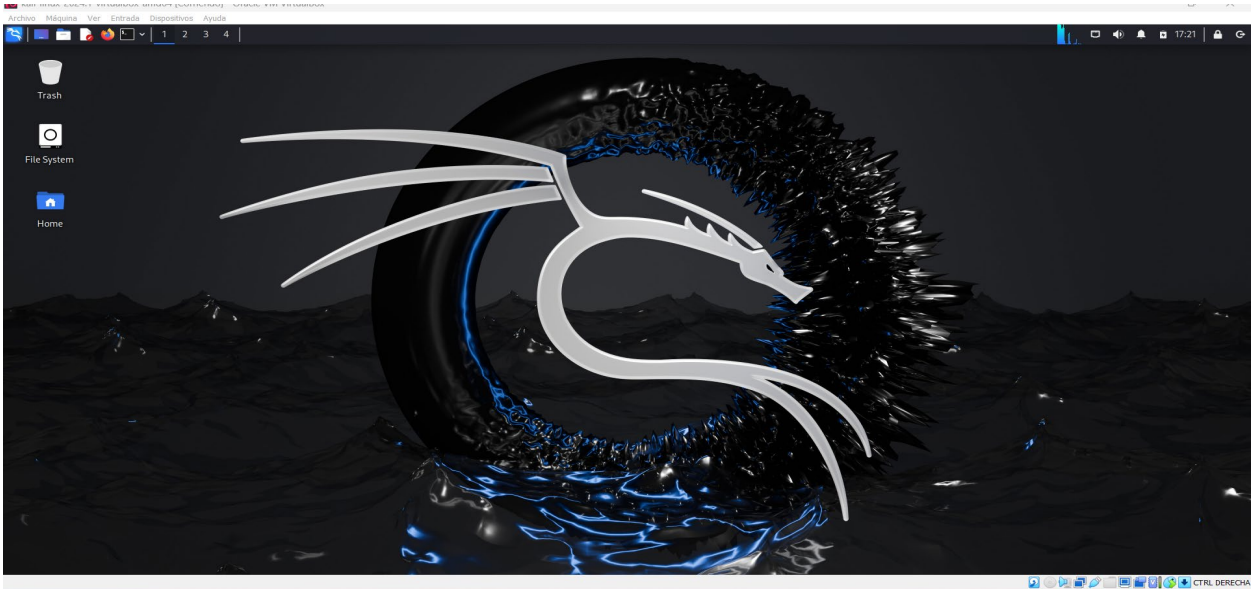
Herramienta VirtualBox



Fuente. Elaboración propia.

Figura 2

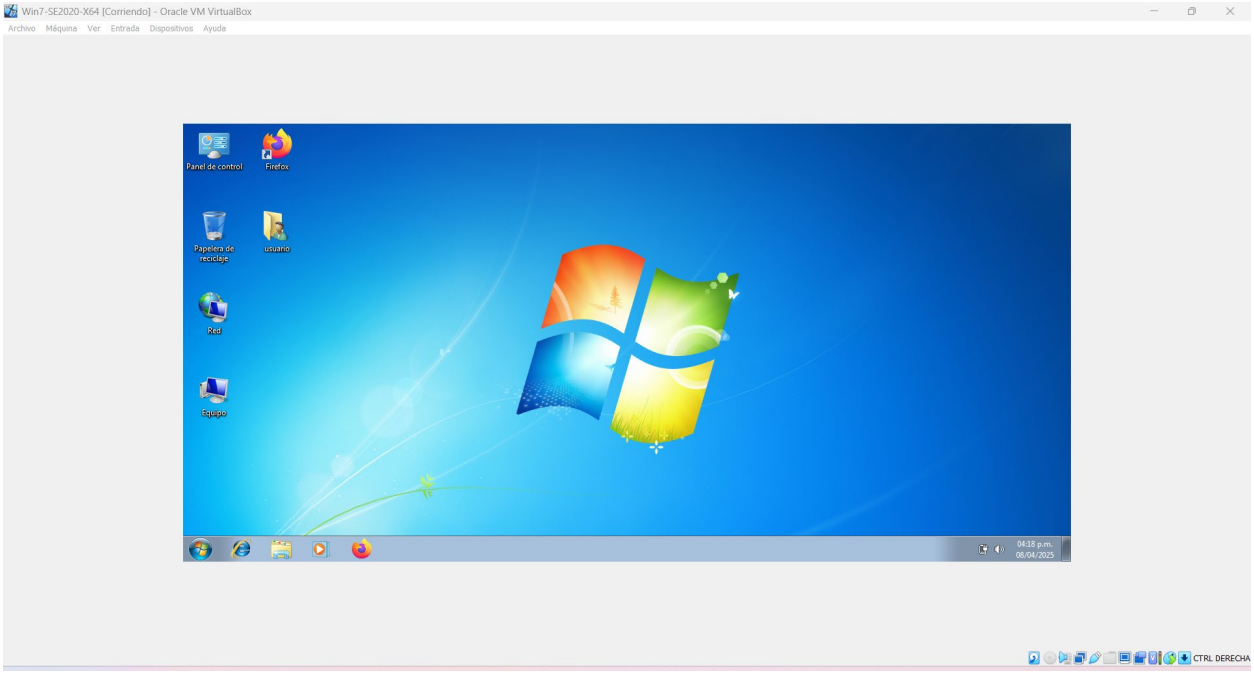
Instalación Sistema Operativo Kali Linux



Fuente. Elaboración propia.

Figura 3

Instalación sistema operativo Windows

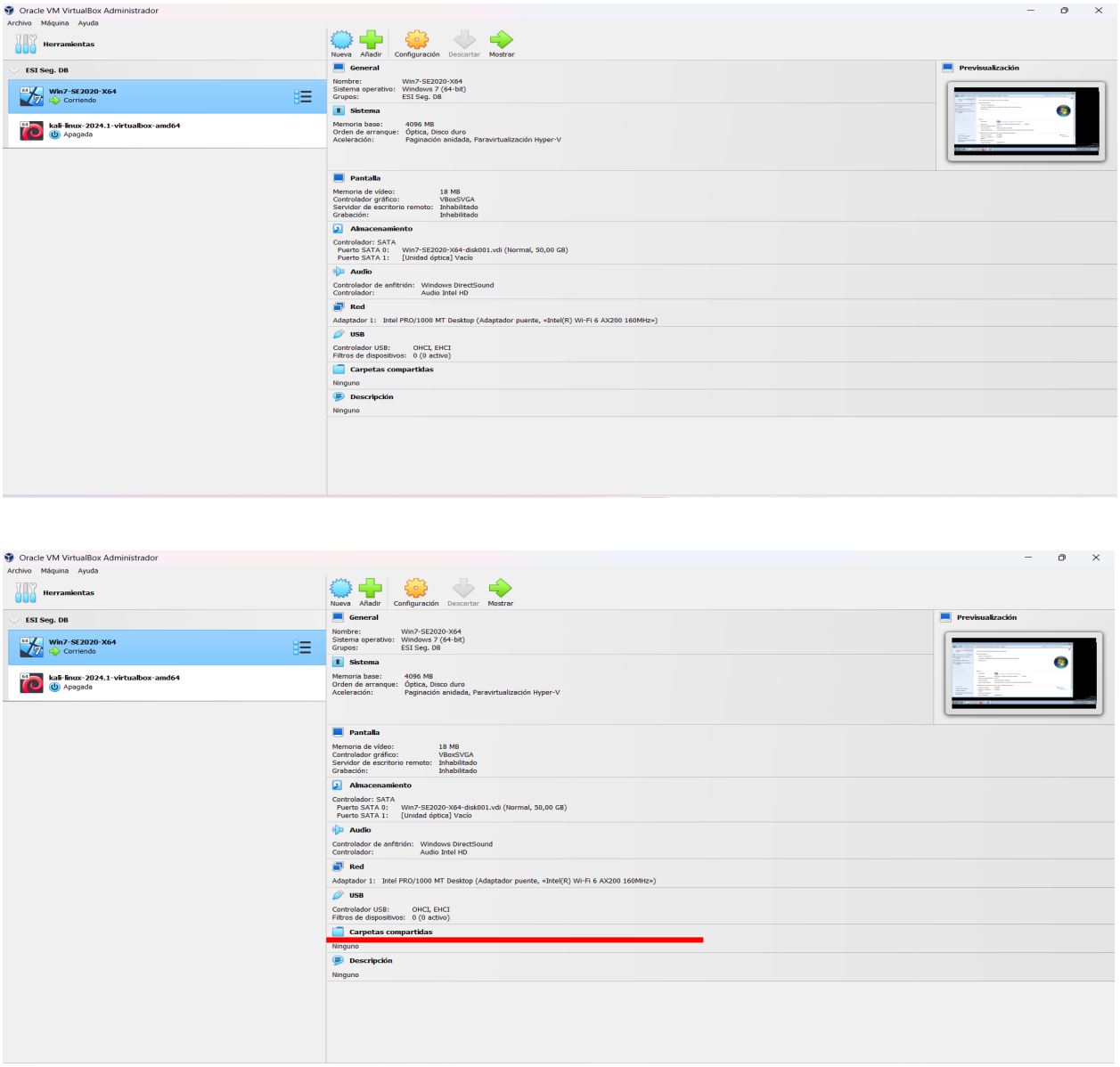


Fuente. Elaboración propia.

En las siguientes imágenes se logra evidenciar que tanto la maquina Windows, como la maquina Linux se encuentran configuradas en el adaptador puente, Intel (R) Wi-Fi 6 AX200 160 MHz, teniendo así comunicación entre ambas maquinas.

Figura 4

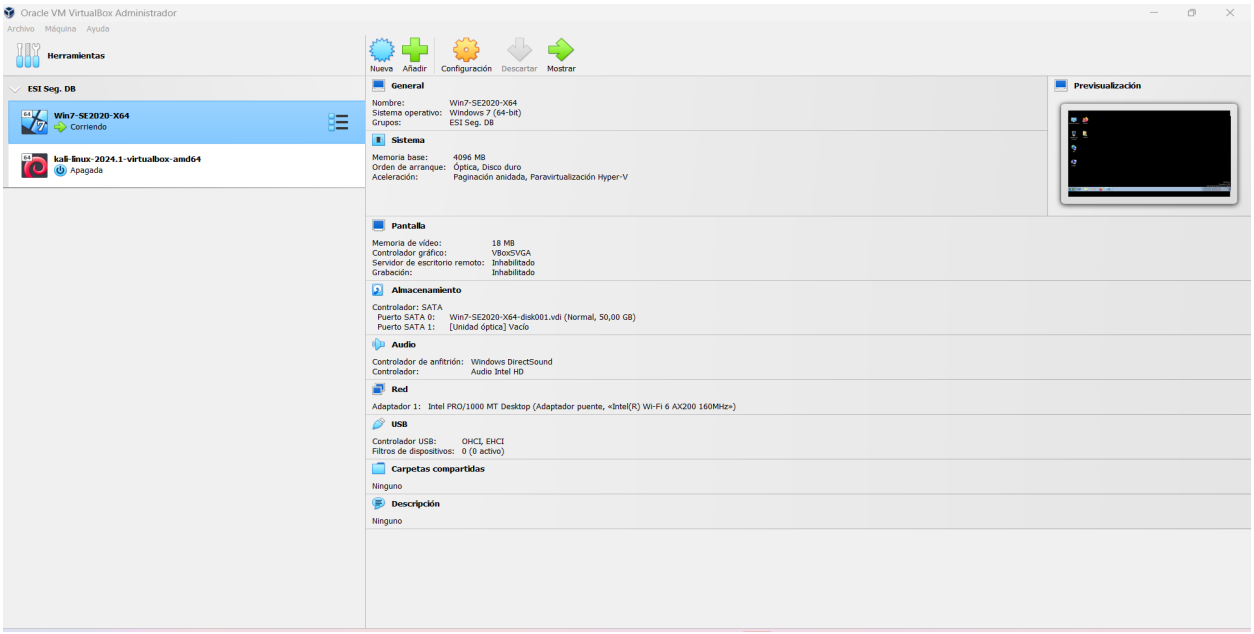
Verificación de la comunicación entre la maquina Linux y Windows



Fuente. Elaboración propia.

Figura 5

Banco de trabajo



Fuente. Elaboración propia.

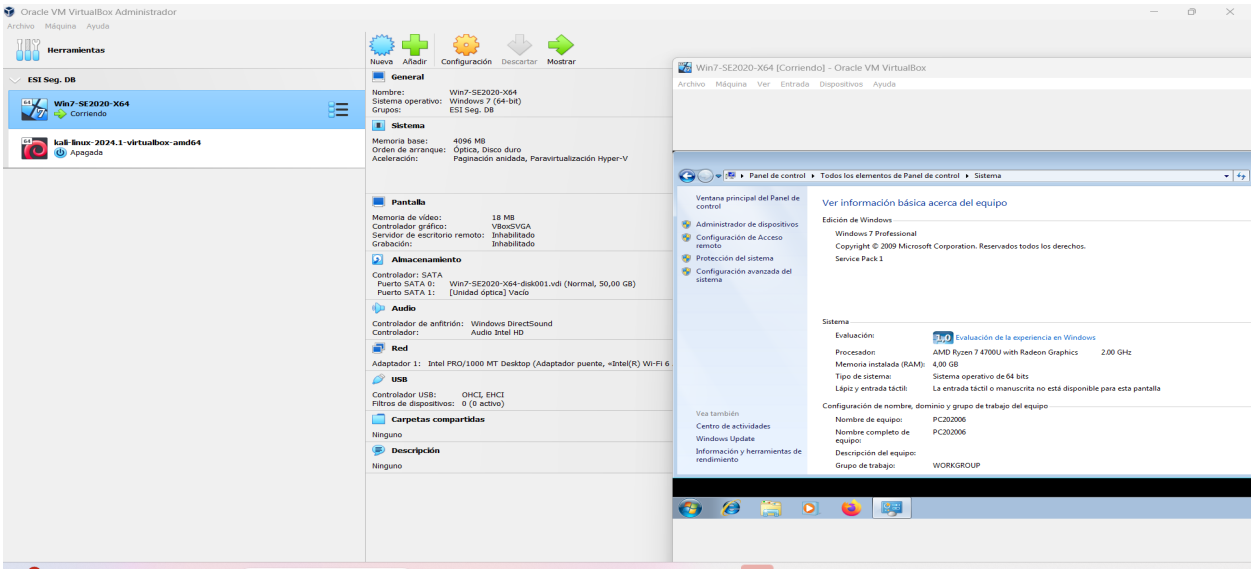
Características de cada maquina

La máquina Windows posee.

- Un sistema operativo Win7 – SE2020-X64 (bit)
- Una memoria Ram de 4,00 GB
- Un procesador 2.00 GHz

Figura 6

Características de la maquina Windows

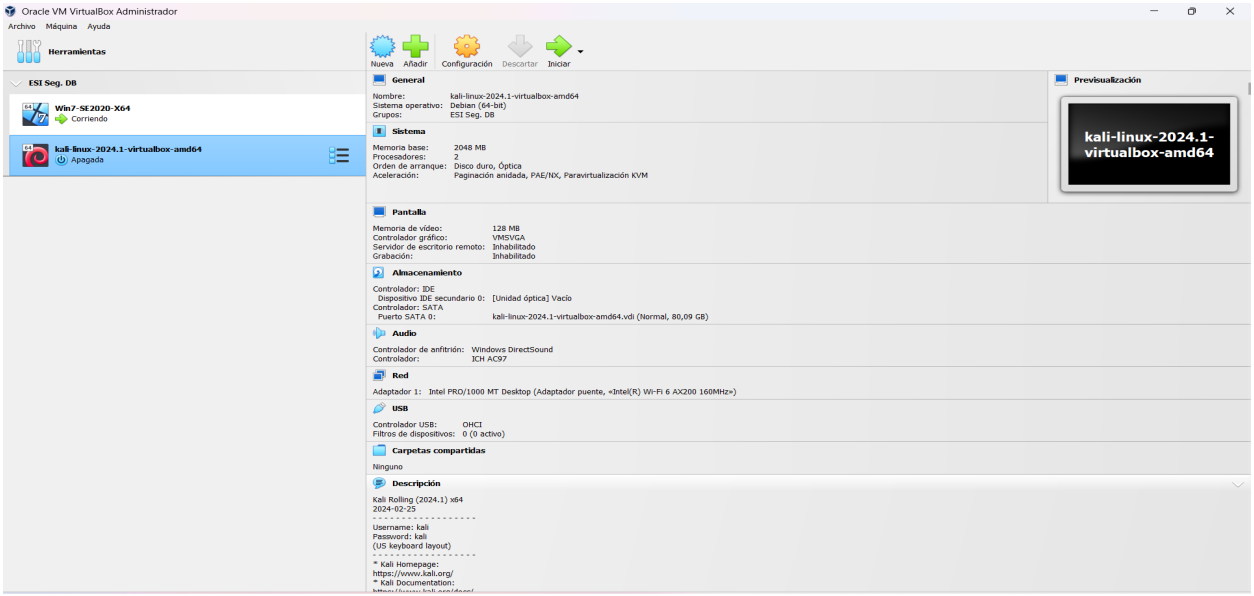


Fuente. Elaboración propia.

La máquina Kali Linux posee Un sistema operativo Debian de 64 bit.

Figura 7

Características de la maquina Linux Sistema operativo

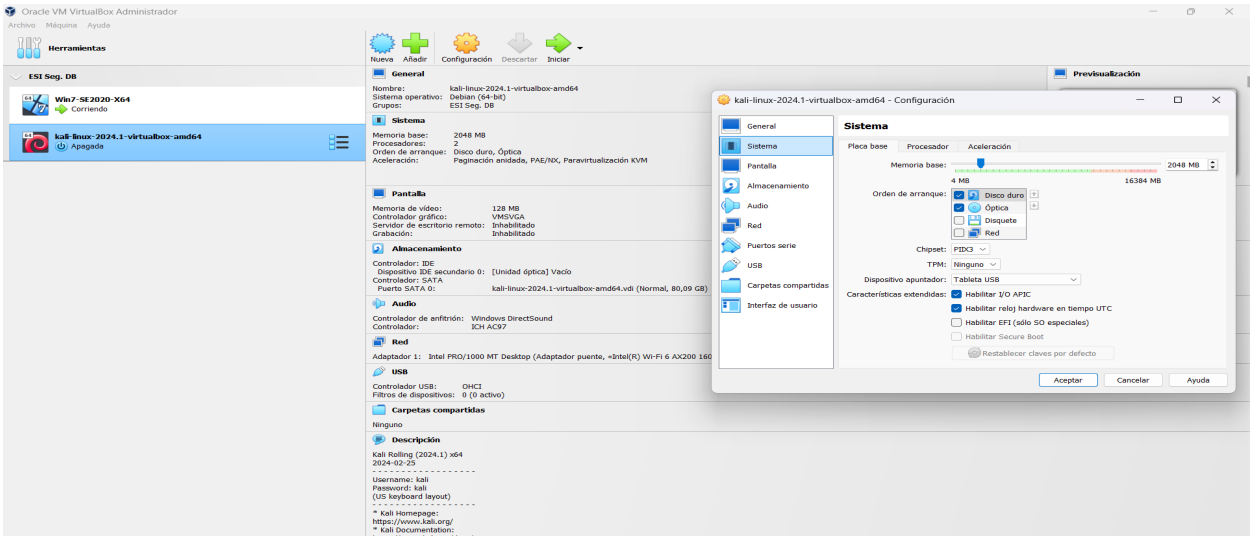


Fuente. Elaboración propia

Una memoria Ram de 4,00 GB

Figura 8

Características de la maquina Linux memoria Ram

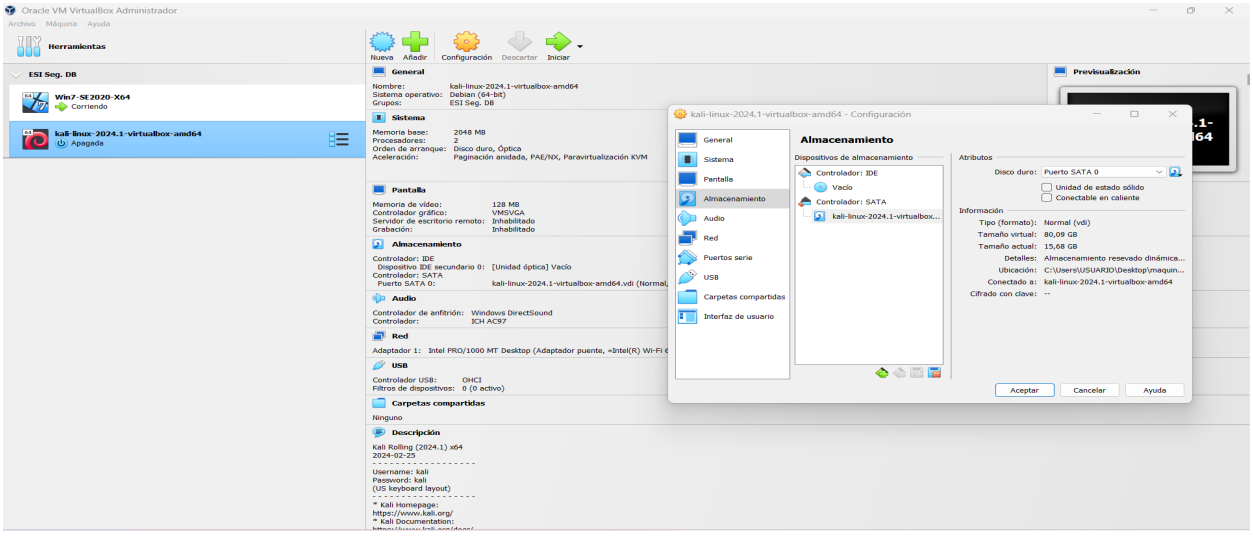


Fuente. Elaboración propia

Un disco duro de 80.09 GB

Figura 9

Características de la maquina Linux Disco duro



Fuente. Elaboración propia

1.5.Ejemplos de casos no éticos evidenciados

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Luego de leer el anexo 2 - escenario 2 y el anexo 3 – Acuerdo, es evidente la existencia de procesos ilegales y no éticos, los cuales deberían ser corregidos. Algunos de estos procesos son.

- En la Segunda clausula Definición de información confidencial, en el inciso número 2 que dice: "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 de información, accesos abusivos a sistemas informáticos".
  parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud"

Siendo CyberFort Technologies una organización la cual presta sus servicios a diferentes empresas no debe cometer este tipo de acciones puesto que, los datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos, son procesos ilegales los cuales son delitos castigados por la ley debido a que violentan los derechos de la privacidad de las personas.

En el momento en que la empresa realice este tipo de practica la persona receptora al firmar este acuerdo y conocer de estos delitos automáticamente se convierten en cómplices por guardar informacion delicada la cual no podría ser divulgada debido a un acuerdo ya firmado.

- En la cuarta clausula Obligaciones de la parte receptora, en el inciso 3 y 4 que dicen:

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

4, Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

En esta cláusula, son evidentes las acciones no éticas que se quieren cometer dado el caso de tener una actividad ilegal en la empresa. Puesto que es claro que toda actividad ilícita observada, ya sea de espionaje, o actividades que afecten o comprometan la integridad de otros, debe ser denunciada ya que es una responsabilidad legal de toda persona dar parte de este tipo de delitos ante la ley.

- En la octava obligación Solución de controversias, donde dice. Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. 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 CyberFort Technologies.

Es notable la injusticia que se presenta en esta cláusula, puesto que busca responsabilizar a la parte rectora de los delitos cometidos en la empresa dejando exenta de responsabilidades a la misma, lo cual es injusto y no ético. En este caso la empresa debe responder por las actividades ilícitas cometidas dentro de la organización junto con todos los involucrados en la misma.

que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Dentro del anexo 3- Acuerdo, se encontraron algunas irregularidades, las cuales teniendo en cuenta la ley 1273 se podrían vulnerar en los siguientes artículos.

Artículo 269A, Artículo 269B, Artículo 269C, Artículo 269D, Artículo 269E, Artículo 269F.

Teniendo en cuenta lo estipulado en el acuerdo de confidencialidad.

- en la segunda clausula, hacen mención, a que los datos chuzados, e intercepción de informacion y accesos abusivos a sistemas informáticos, hacen parte de la información confidencial la cual no se debe revelar.

  Y la ley 1273 en su artículo 269A, el cual hace referencia a el ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO " El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes."

  y el articulo 269C el cual hace referencia a la "INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses."

  Estos artículos penalizan este tipo de actos los cuales son evidentes dentro de las actividades desarrolladas en la empresa CyberFort Technologies.

- En la cláusula número cuatro que se encuentra inscrita en el compromiso de confidencialidad, donde hablan de las no denuncia ante la observancia de actividades sospechosas de espionaje o cualquier otro proceso indebido ocurrido en la empresa. Es vulnerado por la mayoría de los artículos mencionados inicialmente. Es decir:
  el artículo 269a. acceso abusivo a un sistema informático, artículo 269b. obstaculización ilegítima de sistema informático o red de telecomunicación, artículo 269c. interceptación de datos informáticos, artículo 269d. daño informático, artículo 269e. uso de software malicioso y artículo 269f. violación de datos personales.
  Puesto que dentro de las actividades mencionadas que son desarrolladas en la organización, algunas van dirigidas a este tipo de acciones y al cumplir con esta cláusula de no poder denunciar este tipo de actividades, se fomentaría la continuidad y complicidad de estas prácticas, lo que afectaría en gran parte la integridad y funcionamiento de los diferentes sistemas.
- Para finalizar la cláusula número ocho, la cual exime a la empresa CyberFort Technologies de responder por cualquier tipo de actividad indebida y responsabiliza a la parte receptora de responder por estos, es claro que cualquiera de estas actividades podría vulnerar esta ley y exponer a la parte receptora ante procesos legales.

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, ¿usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros.

Luego de realizar un análisis de cada una de las cláusulas estipuladas en el acuerdo de confidencialidad y las implicaciones que esta trae al aceptar este contrato, no sería conveniente aplicar a este trabajo a pesar del sueldo que este propone.

Y mucho más teniendo en cuenta las leyes y obligaciones inscritas en el código de ética Copnia, el cual es quien regula las conductas de los ingenieros.

En este código dentro de sus principios éticos y legales que se encuentran inscrito en la capitulo II, en el artículo 31 DEBERES GENERALES DE LOS PROFESIONALES. Nos dice que Son deberes generales de los profesionales.

b) Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;
f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;

Además de estas en el ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Son prohibiciones especiales a los profesionales respecto de la sociedad:

a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.

En el ARTÍCULO 36. PROHIBICIONES A LOS PROFESIONALES RESPECTO DE LA DIGNIDAD DE SUS PROFESIONES. Son prohibiciones a los profesionales respecto de la dignidad de sus profesiones:

a) Recibir o conceder comisiones, participaciones u otros beneficios ilegales o injustificados con el objeto de gestionar, obtener o acordar designaciones de índole profesional o la encomienda de trabajo profesional.

A pesar de los beneficios económicos que ofrece el contrato de trabajo realizada por CyberFort Technologies y teniendo en cuenta lo establecido en el Código de Ética del COPNIA, de ninguna forma aceptaría esta propuesta. Puesto son claros los objetivos de este código, debido a que busca el actuar con ética profesional, integridad y transparencia ante cualquier circunstancia. De aceptar las condiciones del acuerdo, se estarían infringiendo y violentando muchas leyes, normas y principios.

Deberá analizar el caso problema "Ciberespionaje y Ética en CyberFort Technologies" (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Las empresas de ciberseguridad deben tener acceso solo a la informacion necesaria para cumplir con los objetivos requeridos por una auditoria, donde normalmente el fin de esta es identificar fallas o vulnerabilidades existentes en los sistemas, solo si es estrictamente necesario

se puede dar acceso a informacion un poco más confidencial y por un tiempo estipulado, pero no el acceso a toda la informacion de la empresa como tal.

Para garantizar que el acceso no sea explotado de manera indebida, es necesario establecer reglas, con las que ambas partes deban cumplir, y de no ser así aplicar sanciones legales.

Es importante antes de comenzar la explotación realizar un acuerdo con clausulas claras, donde las partes estén de acuerdo con los estipulado en dicho acuerdo, debe existir supervisión de esta auditoría que garantice que el cumplimiento de los límites establecidos, además de esto brindar un acceso controlado y limitado, donde solo sean involucradas las personas necesarias para cumplir con las actividades y por ultimo y muy importante resaltar la importancia de la ética profesional.

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Para evitar que los empleados de una empresa de ciberseguridad hagan uso indebido de herramientas avanzadas de análisis forense, es importante implementar supervisión continua de las actividades desarrolladas, usando sistemas de monitoreo en tiempo real.

Las auditorías internas son fundamental para mitigar este tipo de actividades, debido a que permiten identificar alguna practica indebida que esté ocurriendo, además de estos observar si se están ocurriendo fallas o incumplimiento de las políticas de la empresa.

Restringir el acceso, brindando privilegios solo a empleados autorizados, además de esto es muy importante la implementación de capacitaciones éticas, donde se deje claro la importancia de esta y las consecuencias de hacer mal uso de estas herramientas.

Con la implementación de este mecanismo es posible que el desempeño de estas herramientas sea con los fines establecidos y así mantener a la empresa fuera de sufrir riesgos de mal uso de con fines personales.

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente

Cuando los gorbiernos y organizaciones descubren que una empresa de ciberseguridad es encontrada cometiendo actos de ciberespionaje, es muy importante que esta realiace una investigacion siendo transparente y actuando con rigor y firmeza, haciendo que las leyes se cumplan y castiguen actos delictivos como el espionaje.

En este proceso se deben tomar medidas como, la finalizacion inmediata de los acuerdos y contratos establecidos, tomando acciones legales que responsabilicen estas acciones.

Para devolver la confianza es esencial que la empresa implemente protocolos de seguridad, los calues sean implementados desde un proceso de seleccoin del personal, mejoras la supervicion del personal contratado, investigar a la empresa antes de realizar la contratacion, garantizar quee esta cumpla con la normatividad y exigencias.

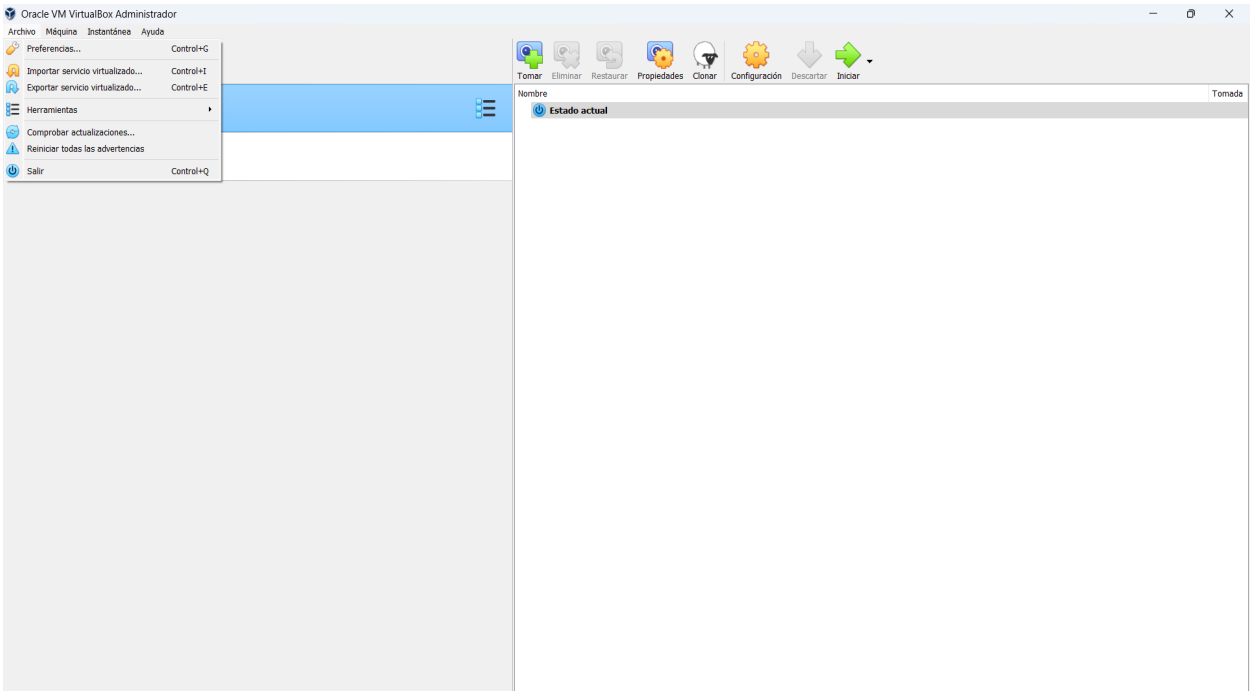
Y por ultimo es muy importante la realizacion de auditorias y capacitaciones, que permitan identificar las vulnerabilidades encontradas y evaluar el estado actual para proponer las mejoras que sean necesarias. Y las capacitaciones son fundamental para comprender cuan imprtante es cumplir con los protocolos y actuar con etica profesional.

1.6. Ejercicio de pentesting o prueba de penetración

Para el desarrollo del ejercicio propuesto fue necesario el uso de una máquina virtual VirtualBox en la cual se realizó el montaje de dos máquinas virtuales, una con sistema operativo Linux y otra con sistema operativo Windows. Fue necesario realizar actualización

Figura 10

Herramienta VirtualBox

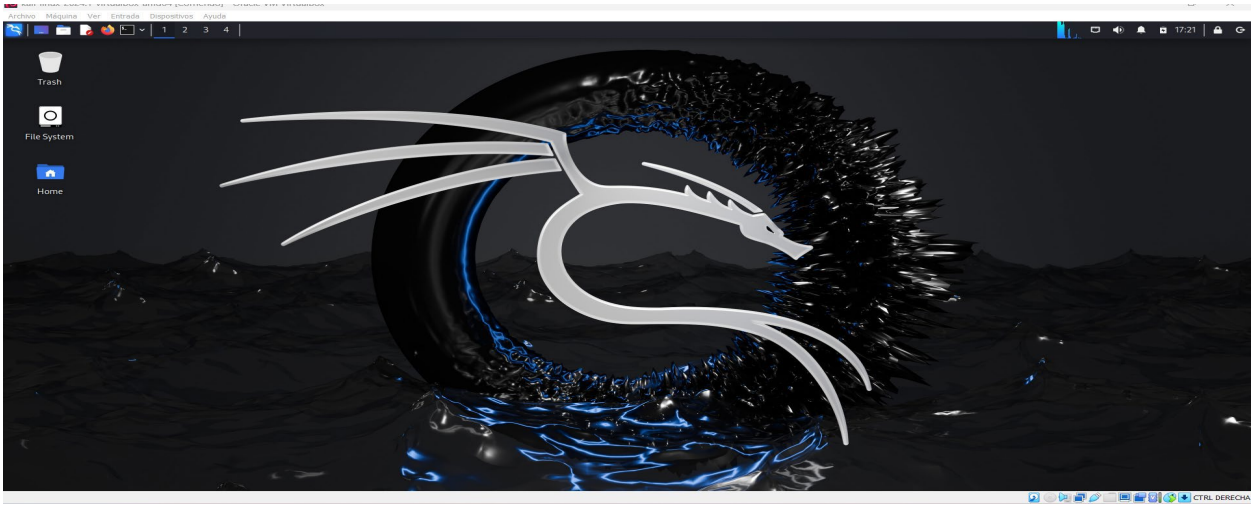


Fuente. Elaboración propia.

Instalación sistema operativo Kali Linux, con la cual se realiza el ataque de pentesting a la maquina Windows.

Figura 11

Instalación sistema operativo Kali Linux

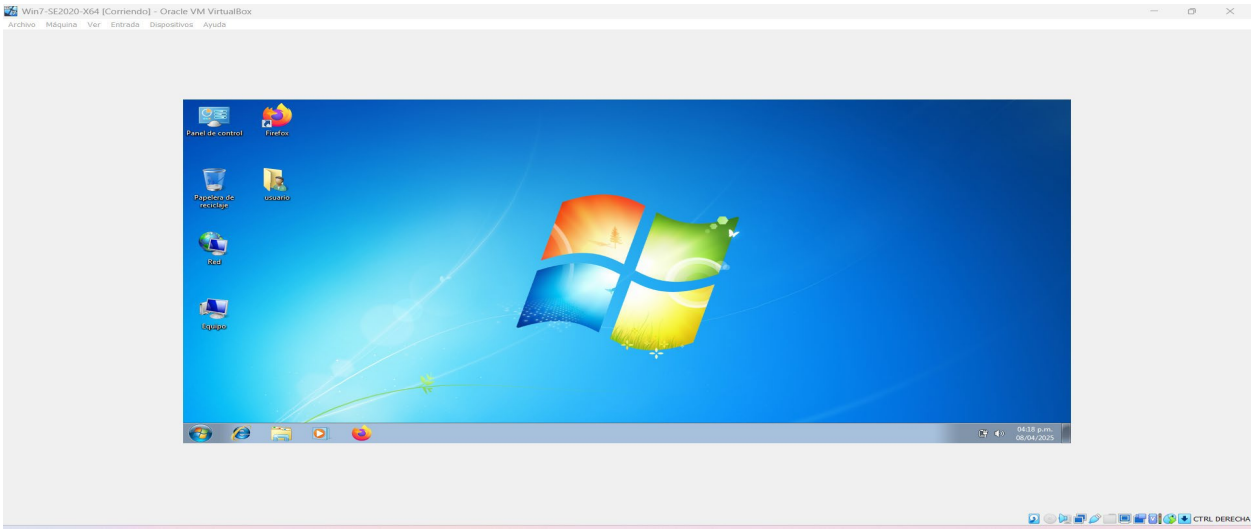


Fuente. Elaboración propia

Instalación sistema operativo Windows, maquina objeto.

Figura 12

Instalación sistema operativo Windows



Fuente. Elaboración propia.

Además, se usó la herramienta **Nmap**, aplicando el comando que se observa en la imagen; con el objetivo de realizar un reconocimiento y lograr obtener informacion de la maquina objeto y así lograr conocer su sistema y funcionamiento.

Figura 13

Ejecución del comando Nmap

Fuente. Elaboración propia

Figura 14

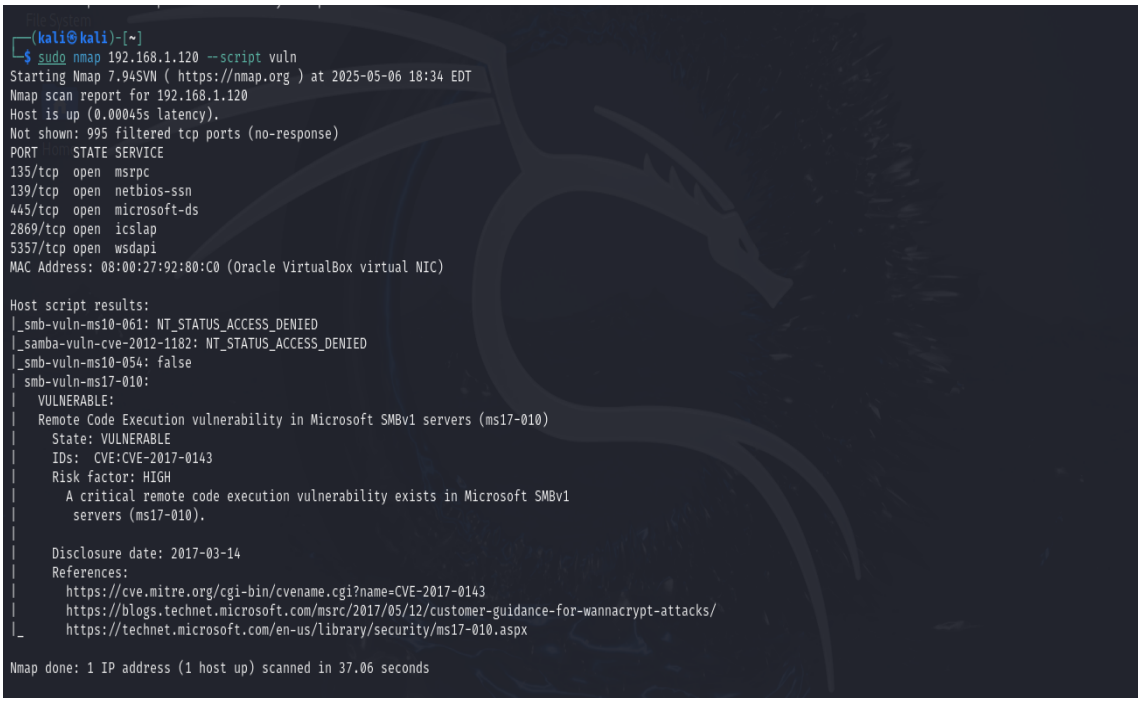
Ejecución del comando Nmap -sV -p-

Fuente. Elaboración propia

Luego se usó sudo nmap 192.168.1.120 --script vuln, con el fin de identificar vulnerabilidades existentes en el sistema, aplicando el comando que se observa en la imagen; en este paso se logran identificar puntos vulnerables que existen en el sistema.

Figura 15

ejecución del comando –script vuln



Fuente- Elaboración propia.

Luego se usó la herramienta metasploit, para así lograr explotar las vulnerabilidades encontradas en el sistema y lograr ingresar al sistema.

Figura 16

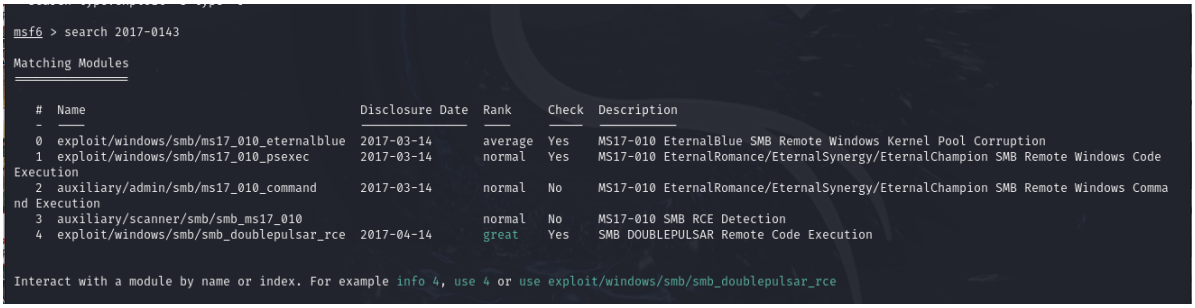
actualización de Metasploit

Fuente. Elaboración propia

Para lograr la exploración fue necesario el uso del comando search junto la vulnerabilidad encontrada, como lo muestra la imagen. "search 2017-0143"

Figura 17

Ejecución del comando search



Fuente. Elaboración propia.

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows.

Para lograr identificar el fallo existente en la maquina Windows fue necesario la identificación de datos importantes que facilitaran una la ejecución del ataque.

- Como primero fue necesario identificar la maquina Windows, para enfocar el análisis en la maquina objeto.
- Luego se da a conocer que existe la presencia de una aplicacion vulnerable en esta máquina, lo que permite sugerir realizar un escaneo para identificar los servicios que esta se ejecuta.
- Además, muestra la posibilidad de que sea muy probable obtener acceso a la maquina a través de la explotación, ejecutando comandos que permitan un ataque exitoso.
- luego de hacer efectivo el ataque, escalar privilegios para de ser posible tomar posesión del usuario principal.
- y al finalizar se sugiere la creación de un usuario con el primer nombre y apellido, luego de hacer efectivo el ataque.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows"? ¿Qué puerto abre la aplicación específica en el anexo?

La herramienta utilizada para lograr identificar los fallos de seguridad que se estaban presentando en la maquina fue Nmap la cual permitió detectar qué servicios estaban corriendo en

la máquina Windows y en qué puertos. Fue de gran ayuda para descubrir si existía una vulnerabilidad expuesta, la cual permitió la entrada a el atacante.

¿Qué puerto abre la aplicación específica en el anexo?

El puerto que da paso a la aplicación es el puerto 445/TCP por el cual se muestra La vulnerabilidad CVE-2017-0143, que afecta al protocolo SMBv1 en diversas versiones de Microsoft Windows.

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows), haga uso de gráficos para explicar el ataque.

Este tipo de ataques, causado por la vulnerabilidad CVE-2017-0143, permite que un atacante remoto pueda ejecutar algún código malicioso o realizar acciones que perjudique la máquina Windows vulnerable enviando paquetes SMBv1 manipulados a través del puerto 445/TCP.

Debido a que este fallo no requiere autenticación, el atacante puede irrumpir en el sistema, logrando afectar en gran medida la seguridad e informacion de esta. A través de este se puede mantener un acceso a la máquina de forma remota, permitiéndole la instalación de malware y la creación de usuarios.

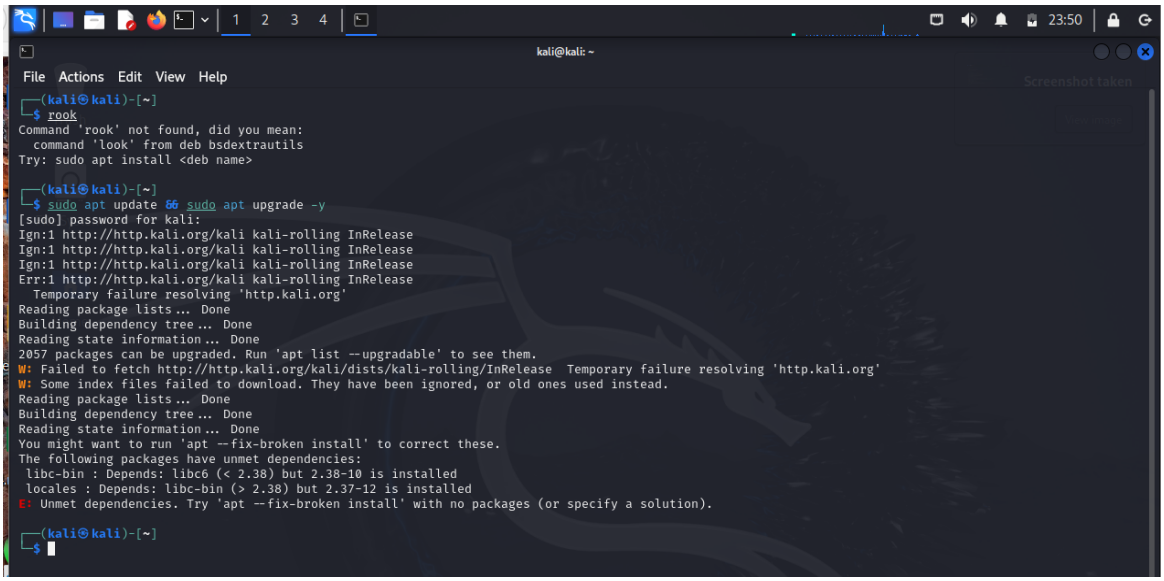
Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Luego de la instalación y configuración de cada una de las maquinas objeto con sudo sistema operativo Windows y maquina principal con sistema operativo Linux. En un entorno de práctica, máquina virtual VirtualBox. Fue necesario realizar actualización.

Y realizamos actualización del sistema ejecutando el comando sudo apt update && sudo apt **upgrade -y** para actualizar el repositorio y todo el sistema.

Figura 18

Actualización del sistema Linux



Fuente. Elaboración propia

Para conocer la ip del ordenador se ejecutó el comando Ip Addr

Figura 19

Comando Ip Addr

Fuente. Elaboración propia.

La cual arrojo la ip del ordenador y de allí tomar como base esa dirección para escanear los puertos.

Luego se ejecuta el comando Nmap para conocer los puertos que se encuentran abiertos en ese segmento de red. Utilizando la dirección sudo Nmap 192.168.1.0/24

Figura 20

Comando Nmap

Fuente. Elaboración propia.

De esta manera se observan las diferentes ip alojada en esta red. Donde se encontraron algunos puertos abiertos.

Se observa que en la dirección 192.168.1.120 existen puertos abiertos mostrando el servicio ejecutado en ellos.

Figura 21

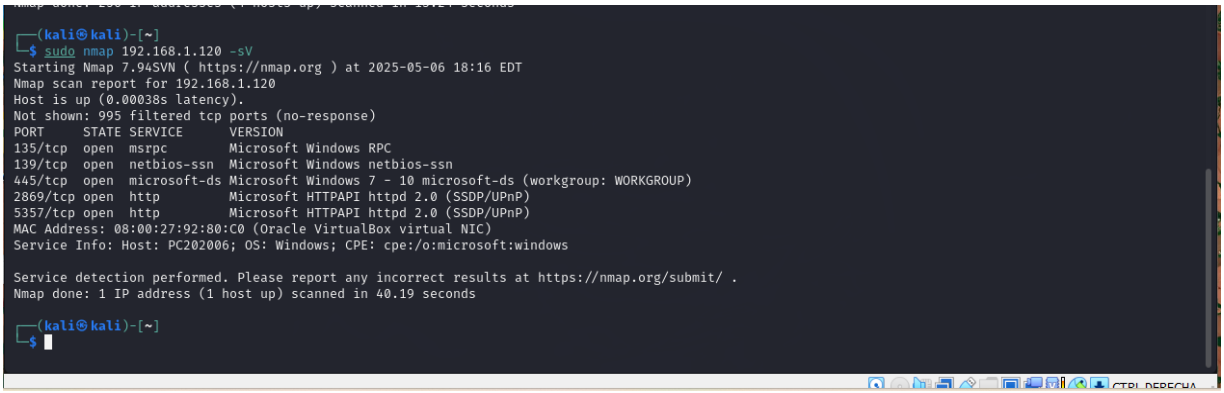
Resultados del comando Nmap

Fuente. Elaboración propia.

Luego de identificar la dirección Ip que contiene puerto abiertos, se procese a realizar un escaneo utilizando el comando sudo Nmap 192**.168.1.120 -sV** para identificar los servicios ejecutados y su versión. Como lo muestra la siguiente imagen

Figura 22

Actualización del comando Nmap

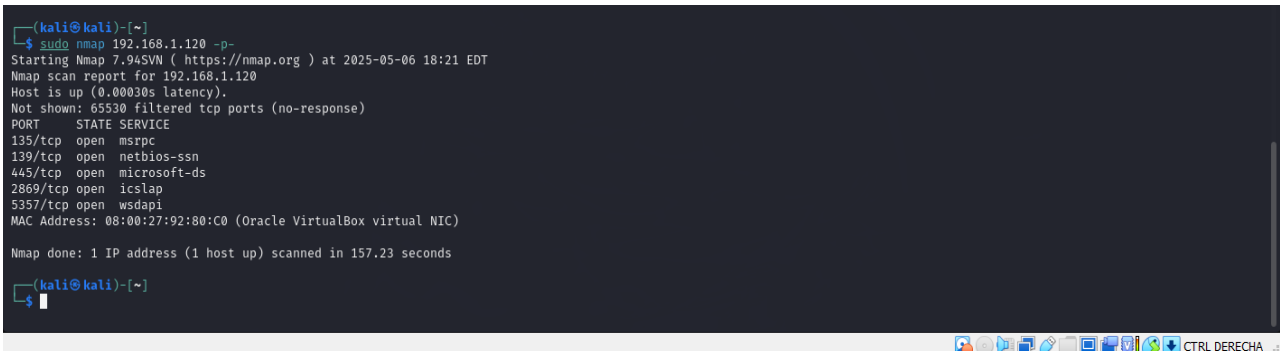


Fuente. Elaboración propia.

Además, se usó el comando sudo Nmap 192**.168.1.120 -p-** el cual permite escanear todos los puertos encontrados en esta dirección Ip, para tener más informacion de la maquina objeto. arrojando el siguiente resultado.

Figura 23

Actualización del comando Nmap

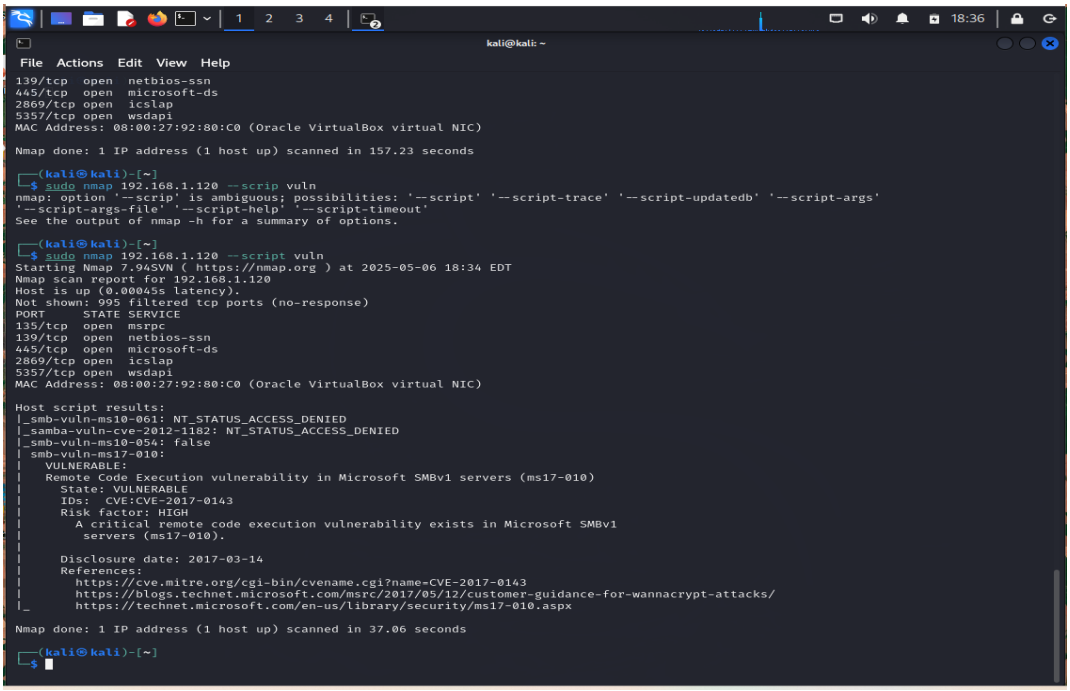


Fuente. Elaboración propia.

Luego obtener informacion necesaria e importante como lo es la dirección Ip, puertos abiertos y haber identificado los servicios, se procede a realizar un Script para identificar las posibles vulnerabilidades que puede haber en estos puertos que se encuentran abiertos. Para este es necesario ejecutar el siguiendo comando. Sudo Nmap 192.168.1.120 --script vuln. El cual arrojo la siguiente informacion.

Figura 24

Comando –script vuln



Fuente. Elaboración propia.

Se encontró una vulnerabilidad identificada **Ids: CVE: CVE-2017-0143** la cual es una vulnerabilidad del “servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario mediante paquetes manipulados, lo que se conoce como

"vulnerabilidad de ejecución remota de código SMB en Windows". Esta vulnerabilidad es diferente de las descritas en CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148." (Mitre.org, 2017).

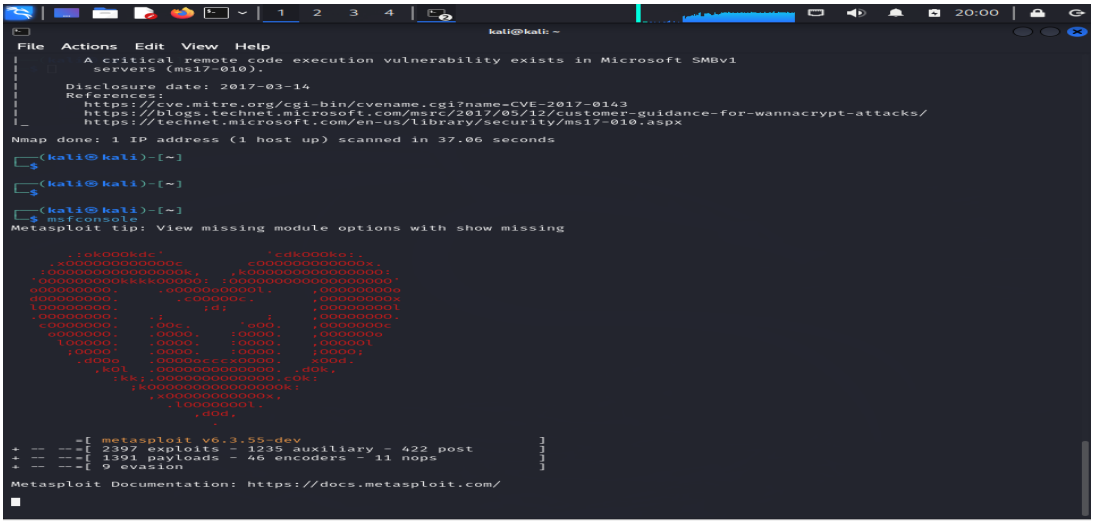
Debido a que fue encontrada una vulnerabilidad, se procede a realizar el respectivo ataque para lograr por medio de esta, conseguir el acceso a la máquina.

Para la realización de dicho proceso es indispensable implementar el comando Metasploit.

Para ejecutar este comando es necesario activarlo primero utilizando el comando msfconsole, como lo muestra la siguiente imagen.

Figura 25

Activación de metasploit



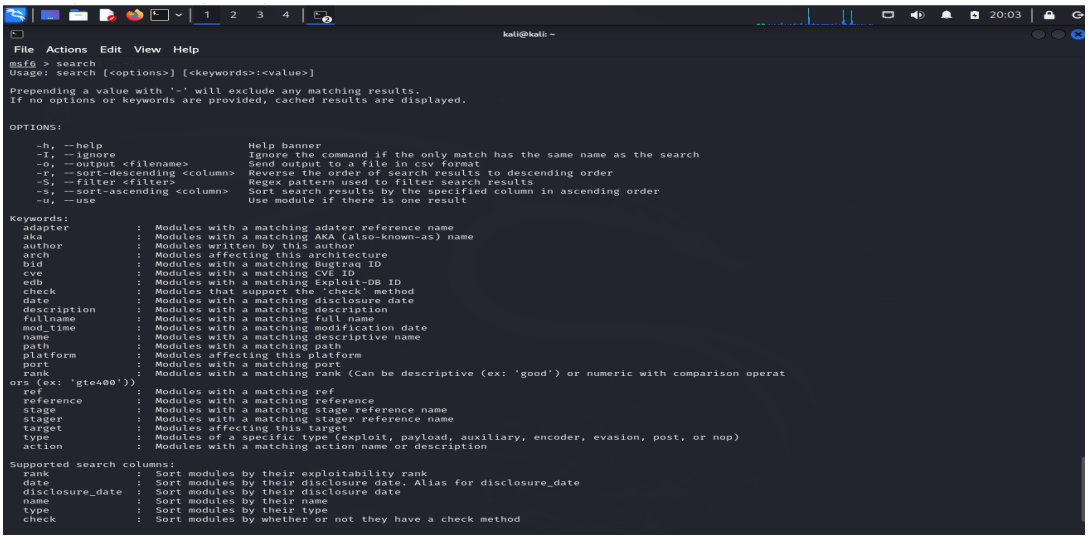
Fuente. Elaboración propia.

De esta manera nos damos cuenta de que ya se encuentra activado el comando Metasploit para ser utilizado.

Luego de este proceso comenzamos la búsqueda de módulos dentro de la estructura, utilizando el comando search, de la siguiente manera.

Figura 26

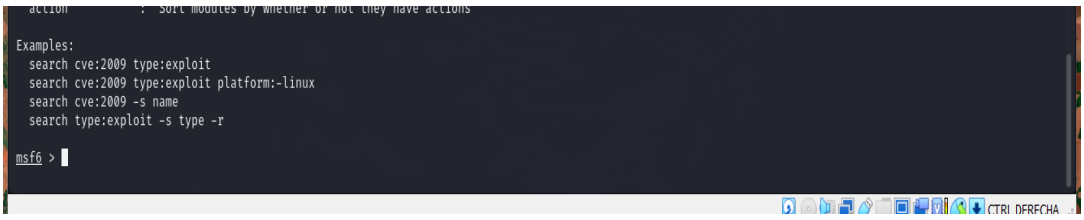
Ejecución del comando search



Fuente. Elaboración propia.

Figura 27

Ejecución del comando search

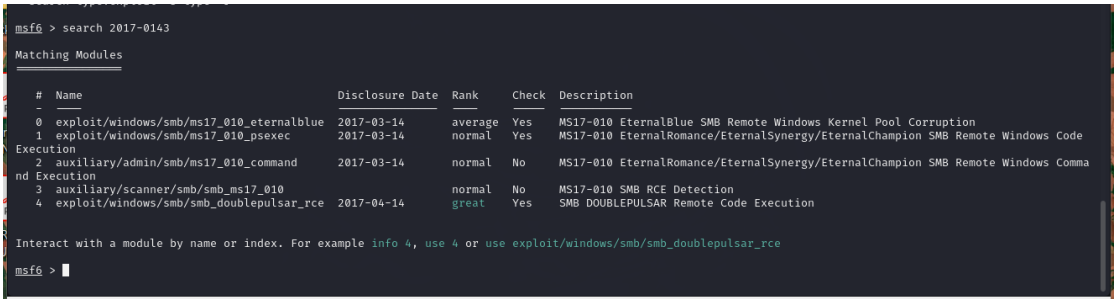


Fuente. Elaboración propia.

A partir de aquí utilizamos el mismo comando “search” pero en este caso adicionamos el numero de la vulnerabilidad de esta forma **search 2017-0143** para que este logre buscar todo lo que se encuentre en ella.

Figura 28

Comando search 2017-0143



Fuente. Elaboración propia.

La cual encontró un módulo auxiliar, el cual nos servirá para la realización del ataque, para interactuar con este módulo es ideal usar el comando use0 el cual tomara la columna y la mostrara completamente.

Figura 29

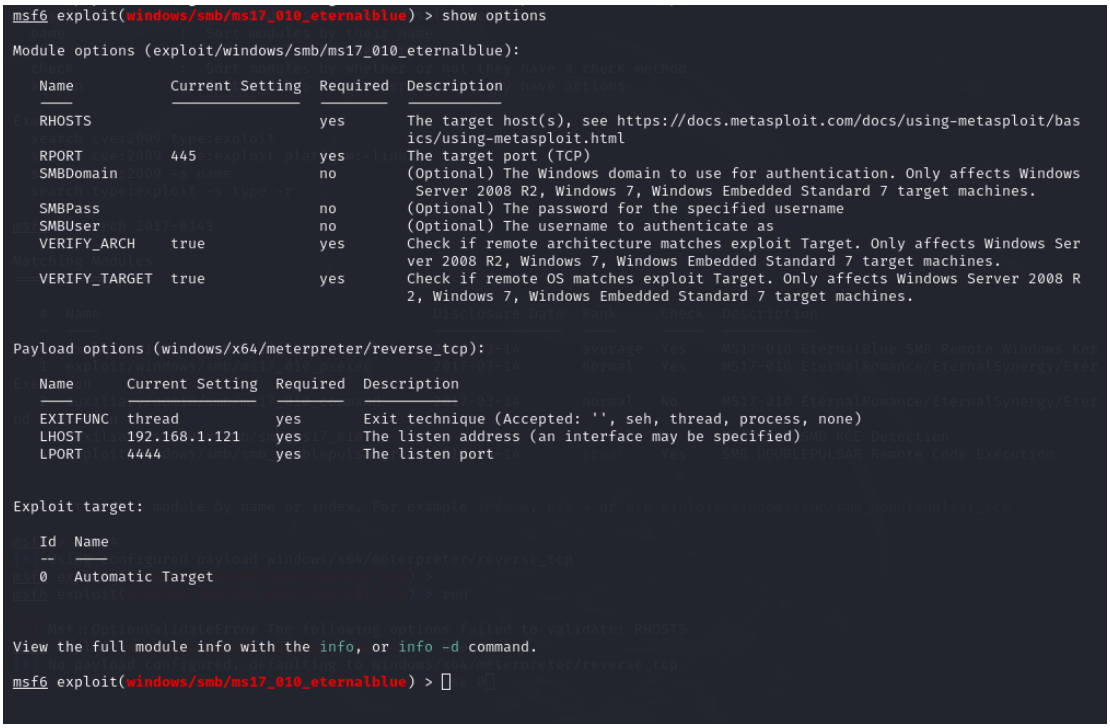
Ejecución del comando use

Fuente. Elaboración propia.

Luego de tener el acceso a esta estructura, proseguimos con la implantación de del comando **show options** el cual nos permite el acceso a la maquita y de esta manera proceder a realizar el ataque.

Figura 30

Ejecución del comando show options



Fuente. Elaboración propia.

De esta manera nos damos cuenta de que ya se encuentra activado el comando Metasploit para ser utilizado.

Luego de este proceso, se procede a enviar el exploit para explotar la vulnerabilidad encontrada durante el escaneo, este proceso fue realizado con la herramienta Metasploit.

1.7.Contención de Ataques Informáticos.

Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Primeramente se debe constatar la Primeramente se debe constatar la veracidad del ataque, verificar que el ataque sea real y ademas indagar hacerca del tipo de ataque. Para asi tomar las medidas adecuadas.

Luego de constatar de que el ataque es real, lo primero que se debe realizar es activar un plan de accion que logre minimizar el ataque y reducir el riesgos de grandes perdidas. Siendo asi se debe realizar un aislamiento del sistema afectado para evitar su propagacion, e iniciar la identificacion del ataque, recolectando todas las evidencias para minimizar el impacto y realizar un analisis profundo de la cituacion.

Para alcanzar resultados positivos es indispensable seguir algunos pasos.

Aislar el sistema. Como primer paso y principal, se debe realizar un aislamiento, desconectando la red, para evitar la propagacion del ataque, e interrumpir cualquier conexión existente de terceros y asi mantener la integridad de la informacion. de esta forma logramos contener el ataque.

Perseverar la evidencia. Luego de aislar el sistema es muy importante capturar el estado del sistema, ya sea atraves de un analisis forence, para identificar el alcance del ataque, que tecnicas fueron usadas para conocer es estado del sistema actualmente.

Identificar la Actividad Sospechosa. En este paso se realiza la identificacion del tipo del ataque, que tantos privilegios se obtuvieron o hasta donde llego su progreso, ademas si aun existe alguna actividad externa la cual se este ejecutando y detener el ataque, bloqueando las conexiones.

Verificar que el ataque ha sido contenido: este paso es muy importante antes de que se reinicien los servicios se debe verificar la contension del ataque, constatando que este haya sido eliminado, y que no existan alertas de nuevas amenazas.

Documentar. Es muy importante documentar el proceso para mejoras futuras y mitigar la posibilidad de nuevas amenazas.

Revisión y actualización de medidas de seguridad. Y finalmente es de gran relevancia la revición y actualización de medidas, que permitan fortalecer la seguridad del sistema y prevenir riesgos futuros.

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team, qué medidas de hardenización propondría para que el ataque no se repita?

Tomando como base la definición de Hardenización y que hace referencia a todas las acciones tomadas para reforzar la seguridad de un sistema y reducir su superficie de ataque. Podemos tener en cuenta algunas medidas.

Control ante privilegios. Tener un control ante las tarear a las que puede acceder cada usuario o los permisos que estos puedan tener, es una forma de reducir en gran medida riegos. Dentro del control de privilegios de puede tener en cuenta.

- Utiliza el control de acceso y los permisos para limitar lo que los usuarios pueden hacer en una base de datos
- Eliminar las cuentas no utilizadas
- Restringe el acceso a las aplicaciones en función de las funciones de los usuarios y del contexto.

Politicas de uso seguro de contraseñas. Esta es de las medidas principalaes que se deben tener en cuenta, puesto a que su buen uso permite o garantiza que los usuarios brinden un manejo adecuadao y protejan debidamente sus cuentass, reduciendo así el riesgo de accesos no autorizados. Para este se debe tener en cuenta.

- Una complejidad que contenga mínimo de 8 a 10 caracteres

- Evitar datos comunes como nombre personal, número de documento o fechas de cumpleaños.
- Incluir mayúsculas, minúsculas, números, caracteres especiales
- Cambiar periódicamente sin repetir contraseñas anteriores
- No guardar por defecto.
- Autenticación de dos factores
- No compartir ni usar la misma contraseña en diferentes cuentas.

Segmentar la red. Segmentar la red limita el alcance de un ataque, aumenta el control y la visibilidad, y refuerza la seguridad global del entorno sin requerir inversiones costosas. Ademas de esto permite aplicar parches y politicas especifica, brindado asi un mejor rendimiento.

Actualización y configuración del sistema. Es de gran importancia abordar la aplicación de parches y la actualización de inmediato. Una herramienta de gestión de parches automatizada y completa es esencial para el fortalecimiento de sistemas. En este paso es muy importante tener en cuenta lo siguiente.

- Asegúrate de que tu firewall está correctamente configurado y de que todas las reglas se auditan y actualizan periódicamente según sea necesario.
- Asegura los puntos de acceso remoto y los usuarios remotos.
- Bloquea los puertos de red innecesarios.

Monitoreo en tiempo real. Al utilizar Software de monitoreo en tiempo real, es posible obtener una visión clara y continua de las actividades que se realizan en el sistema. Esto permite detectar comportamientos anómalos o no autorizados de forma temprana, lo que facilita identificar y detener un posible ataque antes de que cause daño al sistema o la red.

Backups. Los backups o copias de seguridad son una de gran ayuda y a la vez una de las medidas más críticas para proteger la integridad y disponibilidad de la información en cualquier sistema. Su correcta implementación puede marcar la diferencia entre una rápida recuperación y una pérdida catastrófica de datos ante un incidente.

Auditorias internas. Las auditorías ayudan a detectar actividades no autorizadas o el uso indebido de los recursos, así como el incumplimiento de las políticas establecidas. Esto permite corregir fallas o debilidades a tiempo, antes de que se conviertan en riesgos de seguridad mayores. Estas auditorias pueden ser realizadas mes a mes o en el tiempo que se requiera.

Capacitaciones periodicas. La formación del personal es una de las etapas más importantes al implementar medidas de seguridad en un sistema de información. Educar y concientizar a los colaboradores sobre los riesgos y consecuencias de un ciberataque es fundamental para mantener una cultura de seguridad activa y responsable dentro de la organización.

Para fomentar buenas prácticas, es esencial: Realizar simulacros de incidentes reales, que preparen al personal ante situaciones críticas, Impartir capacitaciones periódicas sobre cómo reconocer y manejar vectores de ataque comunes, Generar conciencia sobre las vulnerabilidades existentes y cómo mitigarlas y Reforzar los valores éticos relacionados con el uso adecuado de la información y los recursos tecnológicos. Son medidas de gran ayuda para contar con un personal preparado.

Graccias a el cumplimiento de estos requisitos se lograria contar con un sistema robusto que logre enfrentar riesgos.

¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

La principal diferencia entre un equipo Blue Team y un equipo de respuesta a incidentes es su enfoque y momento de actuación. El Blue Team se encarga de prevenir ataques, implementando medidas de seguridad y monitoreo constante para proteger los sistemas. En cambio, el equipo de respuesta a incidentes actúa una vez que ocurre un incidente, con el objetivo de contener, analizar y recuperar el sistema afectado.

El **blue team** representa a aquellos expertos en ciberseguridad enfocados en proteger las infraestructuras de información contra amenazas digitales. Su principal objetivo es identificar y mitigar vulnerabilidades dentro de los sistemas, garantizando así la seguridad y privacidad de los datos empresariales.

Y el **equipo de respuesta a incidentes**, a veces denominada respuesta a incidentes de ciberseguridad, hace referencia a los procesos y tecnologías de una organización para detectar y responder a ciberamenazas, violaciones de seguridad o ciberataques. Un plan formal de respuesta a incidentes permite a los equipos de ciberseguridad limitar o prevenir daños. (ibm.com, 2024)

Siendo asi El equipo Blue Team se enfoca en proteger y fortalecer la seguridad del sistema para evitar posibles ataques, mientras que el equipo de respuesta a incidentes se encarga de actuar cuando ya ha ocurrido un incidente, gestionando su contención, análisis y recuperación. Ambos equipos son esenciales en la seguridad de los sistemas de información, ya que cumplen funciones distintas pero complementarias. Trabajan de forma coordinada para garantizar una protección efectiva y una respuesta rápida ante cualquier amenaza.

¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS “Center For Internet Security”, usted lo utilizaría para qué fin?

Si dentro de un equipo Blue team se indica trabajar con CIS lo utilizaría con la finalidad de lograr fortalecer la seguridad del sistema, implementando sus estándares y controles de configuración segura.

Siendo CIS una herrameinta la cual es implementada como, un conjunto prescriptivo, priorizado y simplificado de mejores prácticas que puede utilizar para fortalecer su estrategia de ciberseguridad. Hoy en día, miles de profesionales de la ciberseguridad de todo el mundo utilizan los Controles CIS o contribuyen a su desarrollo mediante un proceso de consenso comunitario.

Los controles CIS, permiten.

Simplifique su enfoque de protección contra amenazas. Reduciendo riesgos comunes, como software desactualizado o mala gestión de configuraciones.

Cumplir con las regulaciones de la industria. Facilita el cumplimiento de normal como PCI DSS, HIPAA, RGPD y otras normativas del sector.

Lograr una higiene cibernética esencial. incluyen medidas de seguridad fundamentales que puede utilizar para lograr una ciberseguridad esencial y protegerse contra un ciberataque protegiendo los activos de amenazas comunes..

Traducir la información en acción. Los sistemas y el software modernos son dinámicos por naturaleza. Al implementar los Controles CIS, usted respalda las necesidades cambiantes de sus activos de forma significativa y alinea sus esfuerzos de seguridad con sus objetivos de negocio.

Atender a la ley. Los Controles CIS cumplen con leyes gubernamentales como una forma de demostrar un nivel de seguridad razonable.

Gracias a la implementacion de los controles CIS, se cuenta con guías prácticas que ayudan a establecer configuraciones seguras en diferentes sistemas. Estas recomendaciones permiten evaluar el estado de seguridad del sistema, reducir riesgos, y además, fomentan la capacitación y concientización del personal. Lo que permite finalmente la obtencion de un sistema seguro y eficiente.

Explique y redacte las funciones y características principales de lo que es un SIEM.

La gestión de eventos e información de seguridad, o SIEM, es una solución de seguridad que ayuda a las organizaciones a reconocer y abordar posibles amenazas y vulnerabilidades de seguridad antes de tener la oportunidad de interrumpir las operaciones comerciales.

Los sistemas SIEM ayudan a los equipos de seguridad empresarial a detectar anomalías de comportamiento de los usuarios y utilizan inteligencia artificial (IA) para automatizar muchos de los procesos manuales asociados con la detección de amenazas y la respuesta ante incidentes.

Dentro de las funiones principales de un SIEM podemos mencionar las siguientes

Gestión de registros. SIEM captura datos de eventos de una amplia gama de fuentes en toda la red de una organización. Centraliza y analiza datos de eventos en tiempo real desde sistemas, aplicaciones, usuarios, redes y la nube.

Correlación y analisis de eventos. La correlación de eventos es una parte esencial de cualquier solución SIEM. Identifica patrones y comportamientos sospechosos para detectar amenazas rápidamente.

Monitoreo de incidentes y alertas de seguridad. Debido a que permiten la gestión centralizada de la infraestructura local y basada en la nube, las soluciones SIEM pueden supervisa usuarios y dispositivos, generando alertas ante comportamientos anómalos

Gestión e informes de cumplimiento. Permite Automatizar la recolección de datos necesarios para cumplir con normativas y permitir actuar rápidamente ante amenazas detectadas, mitigando su impacto.

Características principales de un SIEM

Independientemente de cuán grande o pequeña sea una organización, es esencial tomar medidas proactivas para monitorear y mitigar los riesgos de seguridad de TI. Las soluciones SIEM benefician a las compañías de varias maneras.

- Reconocimiento de amenazas en tiempo real.
- Automatización basada en IA.
- Mejora de la eficiencia organizacional.
- Detección de amenazas avanzadas y desconocidas.

Beneficios de SIEM. Dentro de los beneficios que SIEM permite, pordemso mencionar.

- Visibilidad holística.
- Narrativa unificada.
- Detección automática de amenazas.
- Gestión de riesgos.
- Gestión de logs.

- Monitoreo continuo.
- Detección avanzada.
- Búsqueda de amenazas.
- Respuesta ante incidentes.
- Cumplimiento

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Las herramientas de contención de ataques juegan un papel fundamental en la protección de los entornos cibernéticos, ya que permiten limitar el alcance y minimizar el impacto de una amenaza. Estas herramientas actúan bloqueando, aislando o neutralizando el ataque antes de que cause daños mayores. Dentro de estas podemos mencionar algunas como.

Endpoint Detection and Response (EDR).

La detección y respuesta de puntos finales, o EDR, es un software que utiliza análisis en tiempo real y automatización impulsada por IA para proteger a los usuarios finales, los dispositivos de puntos finales y los activos de TI de una organización contra ciberamenazas que superan el software antivirus y otras herramientas de seguridad de puntos finales tradicionales.

EDR recopila datos continuamente de todos los puntos finales de la red: ordenadores de escritorio y portátiles, servidores, dispositivos móviles, dispositivos IoT (Internet de las Cosas) y más. Analiza estos datos en tiempo real para detectar ciberamenazas conocidas o sospechosas y puede responder automáticamente para prevenir o minimizar los daños causados por las amenazas que identifica.

las soluciones EDR generalmente combinan cinco capacidades principales: recopilación continua de datos de puntos finales, análisis y detección de amenazas en tiempo real, respuesta automatizada a amenazas, aislamiento y remediación de amenazas, y soporte para la búsqueda de amenazas

Recopilación continua de datos de puntos finales. EDR recopila continuamente datos (sobre procesos, rendimiento, cambios de configuración, conexiones de red, descargas o transferencias de archivos y datos, comportamiento del usuario final o del dispositivo) de cada dispositivo terminal de la red.

Análisis en tiempo real y detección de amenazas. EDR utiliza análisis avanzados y algoritmos de aprendizaje automático para identificar patrones que indican amenazas conocidas o actividad sospechosa en tiempo real, a medida que se desarrollan.

Respuesta automatizada a amenazas. La automatización es lo que proporciona la "respuesta" —en realidad, la respuesta rápida— en EDR. Basándose en reglas predefinidas establecidas por el equipo de seguridad, o "aprendidas" con el tiempo mediante algoritmos de aprendizaje automático, las soluciones EDR pueden...

- Alertar a los analistas de seguridad sobre amenazas específicas o actividades sospechosas
- Clasificar o priorizar las alertas según la gravedad
- Genere un informe de "retroceso" que rastrea cada paso de un incidente o amenaza en la red, hasta su causa raíz.
- Desconectar un dispositivo terminal o cerrar la sesión de un usuario final de la red
- Detener procesos del sistema o de puntos finales

- Evitar que un punto final ejecute (detone) un archivo o archivo adjunto de correo electrónico malicioso o sospechoso
- Active un software antivirus o antimalware para escanear otros puntos finales de la red en busca de la misma amenaza

Firewalls.

Un firewall es un dispositivo de seguridad de red que monitorea y filtra el tráfico de red entrante y saliente según las políticas de seguridad previamente establecidas de una organización. En su forma más básica, un firewall es esencialmente la barrera que se encuentra entre una red interna privada y la Internet pública. El objetivo principal de un firewall es permitir la entrada de tráfico no amenazante y mantener fuera el tráfico peligroso.

Algunas características integradas, que incluyen:

- Prevención de amenazas de red
- aplicación y control basado en identidad
- Soporte de nube híbrida
- Rendimiento escalable

Existe diferentes tipos de Firewalls como lo son.

- **Filtrado de paquetes.** Una pequeña cantidad de datos se analiza y distribuye de acuerdo con los estándares del filtro.
- **Servicio proxy.** Sistema de seguridad de red que protege mientras filtra mensajes en la capa de aplicación.

- **Stateful inspection firewall.** Filtrado dinámico de paquetes que monitorea las conexiones activas para determinar qué paquetes de red permitir a través del firewall.
- **firewall de última generación (NGFW).** firewall de inspección profunda de paquetes con inspección a nivel de aplicación.

Network Access Control (NAC).

Las soluciones de control de acceso a la red (NAC) permiten a una organización restringir el acceso a la red corporativa de dispositivos y usuarios no autorizados o que no cumplen con las normas. Esto ayuda a garantizar que todos los dispositivos conectados a la red corporativa cumplan con las políticas de seguridad corporativas.

Las soluciones NAC deben incluir las siguientes capacidades principales:

- Visibilidad y creación de perfiles del dispositivo
- Comprobaciones de postura de seguridad
- Acceso restringido a la red:
- Administración de políticas de seguridad:

Conclusiones

Al finalizar este trabajo, se evidencia claramente la importancia de establecer medidas, acciones y estrategias orientadas a mitigar los ataques informáticos y contener su propagación dentro de una organización. La incorporación de un equipo especializado en respuesta ante incidentes representa un recurso clave, ya que facilita el análisis de eventos de seguridad y contribuye a restablecer la operatividad de los servicios afectados. Garantizar la seguridad en un entorno corporativo es fundamental, dado que la reputación y permanencia de la organización dependen en gran medida de ello.

Asimismo, es importante destacar los beneficios que aporta contar con un equipo Blue Team bien preparado, capaz de ofrecer garantías en la protección de los sistemas mediante la implementación de estrategias eficaces para detectar vulnerabilidades, realizar un monitoreo constante y prevenir posibles ataques. La aplicación de buenas prácticas en la gestión organizacional permite consolidar una defensa sólida frente a amenazas cibernéticas y mantener una postura de seguridad constante.

También es esencial reconocer la relevancia de la seguridad de la información. Estar informados y adoptar estrategias alineadas con las metas de la organización son prácticas imprescindibles para alcanzar resultados satisfactorios.

Contar con un equipo de seguridad informática resulta indispensable en cualquier tipo de organización, sin importar su tamaño, ya que garantiza un control adecuado del entorno digital y proporciona estabilidad operativa.

Promover las leyes sobre delitos informáticos es de gran importancia no solo para enfrentar los desafíos legales que se enfrentan en el mundo digital, sino también para para formar

un equipo ético capaz de actuar eficientemente contra el crimen y de esta forma proteger la informacion, y los sistemas ante delitos informáticos.

Cabe señalar que el trabajo conjunto entre los equipos Red Team y Blue Team resulta altamente beneficioso, pues mientras el Red Team identifica vulnerabilidades mediante simulaciones de ataques, el Blue Team se encarga de reforzar los puntos débiles y fortalecer la defensa de manera efectiva.

Finalmente, la colaboración entre ambos equipos mejora significativamente la capacidad de respuesta de la organización frente a incidentes, permitiendo actuar con rapidez y eficacia para proteger los activos críticos y asegurar la continuidad del negocio de forma sostenible.

Recomendaciones

La implementación de los equipos Red Team y Blue Team representa una estrategia fundamental para gestionar y asegurar, de manera efectiva, la protección de los sistemas dentro de una organización.

Desde la perspectiva del Red Team, se busca:

- Definir objetivos concretos que estén alineados con las amenazas más relevantes del entorno actual.
- Ejecutar pruebas éticas bajo un entorno controlado, minimizando riesgos para los sistemas.
- Reproducir ataques sofisticados como amenazas persistentes avanzadas (APT) o campañas de phishing, documentando los hallazgos según su nivel de criticidad.
- Diversificar los escenarios de ataque y realizar ejercicios periódicos que aborden múltiples vectores de riesgo.

En cuanto al Blue Team, sus principales tareas incluyen:

- Utilizar soluciones tecnológicas avanzadas para la supervisión y reacción ante incidentes, como EDR, SIEM o NDR.
- Formar al personal para identificar y responder eficazmente a amenazas complejas.
- Corregir las debilidades descubiertas por el Red Team y mantener los sistemas actualizados frente a nuevas amenazas.

- Ejecutar ejercicios de simulación y adaptar las defensas en función de los aprendizajes obtenidos.

La unión entre ambos equipos permite reforzar significativamente la postura de ciberseguridad, mejorando la capacidad de prevención, detección y respuesta ante ciberataques. Esto contribuye a una mayor solidez de la infraestructura tecnológica y garantiza la continuidad operativa y la confianza a largo plazo en la organización.

Referencias

10 puntos débiles en la ciberseguridad de una empresa. (2022, June 13). Velatia. https://www.velatia.com/es/blog/10-puntos-debiles-en-la-ciberseguridad-de-una-empresa/

Axel. (2024, January 21). Beneficios de Red team y Blue Team en Ciberseguridad. BCNSoluciona, siempre existe una solución. https://www.bcnsoluciona.com/blog/red-team-blue-team-ciberseguridad/

Blue Team: Fortalecer la defensa de una compañía. (2023, April 4). Tarlogic Security; Tarlogic. https://www.tarlogic.com/es/blog/blue-team/

Ciberglosario. (n.d.). Euskadi.eus. Retrieved May 20, 2025, from https://ciberseguridad.euskadi.eus/ciberglosario/equipo-de-respuesta-ante-incidentes

Cilleruelo, C. (2022, June 29). Fases de un pentest. KeepCoding Bootcamps. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad

CIS critical security Controls. (n.d.). CIS; Center for Internet Security. Retrieved May 20, 2025, from https://www.cisecurity.org/controls

Cve - cve-2017-0143. (n.d.). Mitre.org. Retrieved May 20, 2025, from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

de la Información y las Comunicaciones, M. de T. (n.d.). Compilación Jurídica del MINTIC - Ley 1928 de 2018. Ministerio de Tecnologías de la Información y las Comunicaciones. Retrieved May 20, 2025, from https://normograma.mintic.gov.co/mintic/compilacion/docs/ley_1928_2018.htm

Díaz, S. D. (2023, November 29). ¿Eres un Cibernauta? ¡Asume el control de tu experiencia Online! Impacto TIC. https://impactotic.co/innovacion/consumo-digital/estar-conectado-no-lo-hace-un-verdadero-usuario-de-internet/

EDR security - what is endpoint detection and response? (2020, July 24). Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/

Exploit Database: Un recurso valioso para investigadores de seguridad. (2024, January 18). Foros de Informatica, Foro Windows 11. https://www.razorman.net/forodeinformatica/threads/exploit-database-un-recurso-valioso-para-investigadores-de-seguridad.24645/

Guía de referencia de Nmap (Página de manual). (n.d.). Nmap.org. Retrieved May 20, 2025, from https://nmap.org/man/es/index.html

Installing VirtualBox on Kali (host). (n.d.). Kali Linux. Retrieved May 20, 2025, from https://www.kali.org/docs/virtualization/install-virtualbox-host/

Legislación Informática de Colombia. (2016, September 10). Informática Jurídica. https://www.informatica-juridica.com/legislacion/colombia/

Ley 842 de 2003. (n.d.). Gov.co. Retrieved May 20, 2025, from https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Listado completo de herramientas en Kali Linux. (n.d.). Blog Elhacker.net. Retrieved May 20, 2025, from https://blog.elhacker.net/2014/01/kali-linux-listado-completo-de-herramientas-tools.html

Lopez, V. (2024, March 13). Blue team en ciberseguridad: definición, funciones y herramientas. S2GRUPO. https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/

Lozano, P. A. (2023, September 29). Fases del pentesting: Pasos para asegurar tus sistemas. Openwebinars.net. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

ManageEngine. (n.d.). ¿Qué son y cómo implementar los Controles de CIS? Manageengine.com. Retrieved May 20, 2025, from https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

OpenVAS - Escáner de vulnerabilidades de código abierto. (n.d.). Kolibërs Group. Retrieved May 20, 2025, from https://kolibers.com/blog/openvas.html

¿Qué es el control de acceso a la red (NAC)? - Software Check Point. (2022, July 18). Check Point Software. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-access-control-nac/

¿Qué es el pentesting? (2025, enero 27). Ibm.com. https://www.ibm.com/mx-es/topics/penetration-testing

¿Qué es la respuesta a incidentes? (2024, October 11). Ibm.com. https://www.ibm.com/es-es/topics/incident-response

¿Qué es la Seguridad Ofensiva? (2022, November 27). Campus Internacional de Ciberseguridad. https://www.campusciberseguridad.com/blog/item/144-que-es-la-seguirdad-ofensiva

¿Qué es Metasploit Framework y cómo funciona? (2021, December 13). Ciberseguridad. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

¿Qué es MITRE ATT&CK? (n.d.). Anomali.com. Retrieved May 20, 2025, from https://www.anomali.com/es/resources/what-is-mitre-attack-and-how-is-it-useful

¿Qué es SIEM? (2024, November 8). Ibm.com. https://www.ibm.com/es-es/topics/siem

¿Qué es SIEM (gestión de eventos e información de seguridad)? (n.d.). Elastic.co. Retrieved May 20, 2025, from https://www.elastic.co/es/what-is/siem

¿Qué es SIEM (Gestión de eventos e información de seguridad)? - Software Check Point. (2021, February 18). Check Point Software. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/

¿Qué es un equipo azul? - Software Check Point. (2023, May 17). Check Point Software. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-blue-team/

¿Qué es un firewall? (2021, June 16). Check Point Software. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-firewall/

¿Qué son los puntos de referencia de CIS? (2023, May 8). Ibm.com. https://www.ibm.com/mx-es/topics/cis-benchmarks

Unad, W. (2020, August 13). Leyes Informáticas. Universidad Nacional Abierta y a Distancia UNAD - Educación Virtual. https://gpit.unad.edu.co/seguridad-de-la-informacion/leyesinformaticas

What is Endpoint Detection and Response (EDR)? (2025, April 17). Ibm.com. https://www.ibm.com/topics/edr

(N.d.). Gov.Co. Retrieved May 20, 2025, from https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Anexos

Video

https://youtu.be/pPiHQcodzIo