Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

Jorge Hernán Suaza Rincón

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

A mis padres, que desde otra dimensión de la vida acompañan mi proceso, su legado me acompañará por siempre y su recuerdo siempre será un motivo de superación.

A mi esposa, a quien admiro, que me motivó a iniciar este bonito camino, que es un ejemplo por seguir y que siempre ha hecho parte activa en mi proceso formativo.

Agradecimientos

Expreso mi más sincero agradecimiento a mis compañeros, tutores y directivos de la Universidad Nacional Abierta y a Distancia (UNAD), quienes han sido parte fundamental de este proceso formativo y han contribuido significativamente a mi crecimiento académico y profesional. Su acompañamiento, orientación y apoyo constante han sido esenciales en cada etapa de este camino.

De igual manera, agradezco a los autores y profesionales que, a través del material educativo consultado, han aportado valiosamente al fortalecimiento de mis conocimientos, permitiéndome enriquecer mi formación como profesional como futuro especialista.

Resumen

La ciberseguridad se ha consolidado como un componente estratégico fundamental para la protección de los activos digitales de las organizaciones frente al creciente aumento de amenazas y ataques informáticos. En este contexto, los equipos red team y blue team desempeñan un papel esencial en la evaluación, fortalecimiento y defensa de la infraestructura tecnológica mediante la aplicación de capacidades técnicas, tácticas y operativas especializadas. El presente trabajo aborda los fundamentos de las operaciones red team y blue team, describiendo sus funciones, metodologías y herramientas empleadas en la identificación de vulnerabilidades, la simulación de ataques y la protección de los sistemas de información. Asimismo, se analiza el marco legal colombiano aplicable a los delitos informáticos y a la protección de datos personales, destacando las principales disposiciones normativas que regulan el tratamiento de la información y las responsabilidades derivadas de incidentes de seguridad. De igual manera, se examinan los principios éticos y el marco normativo que orientan el ejercicio profesional en ciberseguridad, enfatizando la importancia de actuar bajo criterios de legalidad, responsabilidad y respeto por la privacidad y los derechos de los usuarios. Finalmente, se estudian los procesos de respuesta y contención ante incidentes de ciberseguridad, incluyendo las actividades de detección, análisis, mitigación, recuperación y mejora continua, las cuales resultan esenciales para reducir el impacto de los ataques y fortalecer la resiliencia organizacional.

***Palabras clave*:** Blue team, ciberseguridad, normatividad, pentesting, red team.

Abstract

Cybersecurity has become a fundamental strategic component for protecting organizations' digital assets against the increasing number of cyber threats and attacks. In this context, red teams and blue teams play an essential role in assessing, strengthening, and defending technological infrastructure through the application of specialized technical, tactical, and operational capabilities. This paper addresses the fundamentals of red team and blue team operations, describing their functions, methodologies, and tools used in identifying vulnerabilities, simulating attacks, and protecting information systems. It also analyzes the Colombian legal framework applicable to cybercrimes and the protection of personal data, highlighting the main regulations governing information processing and the responsibilities arising from security incidents. Similarly, it examines the ethical principles and regulatory framework that guide professional practice in cybersecurity, emphasizing the importance of acting in accordance with legality, responsibility, and respect for privacy and user rights. Finally, the processes of response and containment to cybersecurity incidents are studied, including the activities of detection, analysis, mitigation, recovery and continuous improvement, which are essential to reduce the impact of attacks and strengthen organizational resilience.

Keywords: Blue team, cybersecurity, regulations, pentesting, red team.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

ACL (Access Control List):

Reglas que permiten o restringen el acceso a recursos de red, sistemas o aplicaciones según criterios previamente definidos por una organización.

Análisis forense digital:

Proceso de identificación, preservación, recolección y análisis de evidencia digital con el fin de determinar cómo ocurrió un incidente de seguridad.

Blue Team:

Equipo encargado de proteger, monitorear y defender la infraestructura tecnológica de una organización frente a amenazas y ataques informáticos.

Cadena de custodia:

Procedimiento documentado que garantiza la integridad y trazabilidad de las evidencias digitales desde su recolección hasta su presentación.

Ciberespionaje:

Obtención no autorizada de información sensible mediante técnicas informáticas con fines estratégicos, económicos o para afectar la reputación de una persona u organización.

CIS (Center for Internet Security):

Organización que desarrolla controles y guías de seguridad reconocidos internacionalmente para fortalecer la protección de sistemas y redes.

Confidencialidad:

Principio de seguridad que garantiza que la información solo sea accesible para personas o entidades autorizadas.

CVE (Common Vulnerabilities and Exposures):

Sistema de identificación estandarizado utilizado para catalogar vulnerabilidades y fallos de seguridad de software y hardware públicamente conocidos. Funciona como un identificador único global que permite a los equipos especializados referirse exactamente al mismo fallo de seguridad en cualquier parte del mundo .

EDR (Endpoint Detection and Response):

Solución de seguridad diseñada para detectar, analizar y contener amenazas que afectan estaciones de trabajo (Host) y otros dispositivos finales.

Escalada de privilegios:

Técnica mediante la cual un atacante obtiene permisos superiores a los originalmente asignados dentro de un sistema.

Firewall:

Dispositivo o software que controla el tráfico de red entrante y saliente mediante reglas de seguridad previamente configuradas.

FTK Imager:

Herramienta forense utilizada para adquirir y preservar copias exactas de discos, particiones y otros medios de almacenamiento digital.

Hardening:

Conjunto de medidas técnicas orientadas a reducir la superficie de ataque de un sistema mediante configuraciones seguras y eliminación de servicios innecesarios.

Hash:

Valor único generado a partir de datos mediante algoritmos matemáticos, utilizado para verificar la integridad y autenticidad de la información.

HFS (HTTP File Server):

Aplicación que permite compartir archivos mediante el protocolo HTTP y que puede convertirse en un riesgo de seguridad cuando presenta vulnerabilidades conocidas.

Host:

Cualquier dispositivo conectado a una red que puede enviar y recibir datos. Pueden ser: Computadoras, servidores, dispositivos móviles, dispositivos IoT, etc.

IDS (Intrusion Detection System):

Sistema que monitorea eventos y tráfico de red para identificar actividades sospechosas o ataques potenciales.

IOC (Indicator of Compromise):

Evidencia técnica que permite inferir que un sistema ha sido comprometido o utilizado de manera maliciosa.

IPS (Intrusion Prevention System):

Tecnología capaz de detectar y bloquear automáticamente actividades maliciosas antes de que afecten los sistemas protegidos.

ISO/IEC 27001:

Norma internacional que establece requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información.

ISO/IEC 27701:

Norma internacional orientada a la gestión de privacidad y protección de datos personales.

Kali Linux:

Distribución de Linux especializada en pruebas de penetración, análisis de vulnerabilidades y evaluación de seguridad informática.

Logs:

Registros generados por sistemas, aplicaciones o dispositivos que almacenan eventos y actividades relevantes para auditoría y monitoreo.

Malware:

Software diseñado para ejecutar acciones maliciosas, como robo de información, alteración de sistemas o interrupción de servicios.

Metasploit Framework:

Plataforma de pruebas de seguridad utilizada para validar vulnerabilidades y evaluar riesgos en entornos autorizados.

Movimiento lateral:

Desplazamiento de un atacante desde un sistema comprometido hacia otros equipos dentro de una misma organización.

NAC (Network Access Control):

Tecnología que controla el acceso de dispositivos a la red según políticas de seguridad establecidas.

NIST (National Institute of Standards and Technology):

Organismo estadounidense que desarrolla marcos de referencia y buenas prácticas ampliamente utilizadas en ciberseguridad.

Nmap (Network Mapper):

Herramienta de reconocimiento y análisis que permite identificar hosts, puertos abiertos y servicios disponibles en una red.

Pentesting (Prueba de penetración):

Evaluación controlada y autorizada que busca identificar vulnerabilidades explotables en sistemas, redes o aplicaciones.

Pivoting:

Técnica utilizada para acceder a redes o sistemas adicionales a través de un equipo previamente comprometido.

ProxyChains:

Herramienta que permite redirigir conexiones de red a través de proxys para acceder a recursos ubicados en otras redes.

Ransomware:

Tipo de malware que bloquea o cifra información para exigir un pago a cambio de su recuperación.

RCE (Remote Code Execution):

Vulnerabilidad que permite ejecutar instrucciones o programas en un sistema remoto sin autorización.

Red Team:

Equipo especializado en simular ataques reales con el objetivo de evaluar la capacidad defensiva de una organización.

Respuesta a incidentes:

Conjunto de actividades destinadas a detectar, contener, erradicar y recuperar sistemas afectados por eventos de seguridad.

Segmentación de red:

Técnica que divide una infraestructura en múltiples segmentos para limitar la propagación de amenazas y mejorar el control de acceso.

SIEM (Security Information and Event Management):

Plataforma que centraliza, correlaciona y analiza eventos de seguridad procedentes de diferentes fuentes tecnológicas.

SMB (Server Message Block):

Protocolo utilizado para compartir archivos, impresoras y otros recursos entre equipos conectados a una red.

SMBv1:

Versión antigua del protocolo SMB que presenta múltiples vulnerabilidades de seguridad y actualmente se considera obsoleta.

SOC (Security Operations Center):

Centro especializado encargado de supervisar, detectar y responder a incidentes de seguridad de manera continua.

Sysmon (System Monitor):

Herramienta de monitoreo avanzado para Windows que registra eventos detallados relacionados con actividades del sistema.

UAC (User Account Control):

Mecanismo de seguridad de Windows que ayuda a prevenir cambios no autorizados mediante la validación de privilegios.

VLAN (Virtual Local Area Network):

Segmentación lógica de una red física que permite separar dispositivos y controlar mejor el tráfico.

Volatility:

Herramienta de análisis forense enfocada en el estudio de memoria RAM para identificar procesos, conexiones y evidencias de ataques.

Vulnerabilidad:

Debilidad presente en un sistema, aplicación o configuración que puede ser aprovechada para comprometer la seguridad.

WannaCry:

Malware de tipo ransomware que aprovechó la vulnerabilidad MS17-010 para propagarse masivamente en sistemas Windows.

Wireshark:

Analizador de protocolos de red utilizado para capturar e inspeccionar tráfico con fines de diagnóstico y análisis de seguridad.

Zero Trust:

Modelo de seguridad basado en la premisa de no confiar automáticamente en ningún usuario o dispositivo, independientemente de su ubicación dentro o fuera de la red.

Introducción

La ciberseguridad se ha consolidado como un componente estratégico dentro de las organizaciones modernas, debido al incremento constante de amenazas informáticas que comprometen la confidencialidad, integridad y disponibilidad de la información. En un entorno altamente digitalizado, donde los procesos operativos, administrativos y estratégicos dependen de infraestructuras tecnológicas interconectadas, resulta indispensable comprender tanto las técnicas utilizadas por los atacantes como los mecanismos de defensa orientados a prevenir, detectar, contener y responder ante incidentes de seguridad.

El presente informe desarrolla de manera integral conceptos, metodologías y prácticas relacionadas con las operaciones de red team y blue team, mediante el análisis de un escenario práctico basado en el caso de SecureNova Labs. Para ello, se implementó un laboratorio virtual conformado por una máquina Kali Linux y dos sistemas Windows denominados Host A y Host B, configurados en diferentes segmentos de red con el fin de simular una infraestructura corporativa vulnerable a ataques reales.

Dentro del ejercicio práctico se realizaron actividades de reconocimiento, escaneo de puertos y servicios, identificación de vulnerabilidades, explotación controlada y movimiento lateral entre segmentos de red. Particularmente, se identificó la exposición de un servicio vulnerable asociado a HFS (HTTP File Server), el cual permitió la ejecución remota de comandos y el establecimiento de una sesión Meterpreter sobre Host A. Posteriormente, mediante técnicas de pivoting y el uso de herramientas como ProxyChains, fue posible acceder a Host B, demostrando cómo una vulnerabilidad inicial puede escalar hasta comprometer múltiples activos dentro de una infraestructura tecnológica.

Desde la perspectiva defensiva, el informe aborda el análisis de respuesta a incidentes desde el enfoque blue team, incluyendo la identificación de indicadores de compromiso,

preservación de evidencia digital, aislamiento de sistemas comprometidos, hardening, segmentación de red e implementación de controles avanzados de monitoreo como SIEM, EDR e IDS/IPS. Estas medidas buscan reducir la superficie de ataque y fortalecer la capacidad de detección temprana y respuesta organizacional frente a amenazas cibernéticas.

Adicionalmente, el documento incorpora una reflexión sobre los aspectos éticos, legales y profesionales asociados al ejercicio de la ciberseguridad, analizando las implicaciones del marco normativo colombiano en relación con delitos informáticos, protección de datos personales, manejo de evidencias digitales y límites legales de las actividades ofensivas y defensivas. De igual forma, se examina el papel del profesional en ciberseguridad desde la perspectiva del Código de Ética del COPNIA.

Finalmente, este trabajo busca integrar conocimientos técnicos, normativos y estratégicos que permitan comprender la importancia de articular capacidades ofensivas y defensivas dentro de una estrategia integral de ciberseguridad, orientada a fortalecer la resiliencia tecnológica de las organizaciones frente a amenazas cada vez más sofisticadas.

Justificación

La creciente dependencia de las organizaciones respecto a sistemas de información, redes y plataformas digitales ha incrementado significativamente la exposición a amenazas cibernéticas capaces de comprometer activos críticos de información. En este contexto, resulta fundamental que los profesionales del área tecnológica, especialmente aquellos enfocados en seguridad informática, desarrollen competencias técnicas, analíticas y estratégicas que les permitan comprender tanto las técnicas ofensivas utilizadas por actores maliciosos como los mecanismos defensivos necesarios para proteger la infraestructura tecnológica.

La realización de este tipo de trabajo permite fortalecer conocimientos teóricos y prácticos relacionados con la ciberseguridad, mediante la aplicación de metodologías de análisis ofensivo y defensivo en entornos controlados. A través del estudio de actividades asociadas a equipos red team y blue team, se adquieren habilidades para identificar vulnerabilidades, evaluar riesgos, comprender el impacto de posibles ataques informáticos y diseñar mecanismos efectivos de prevención, detección, contención y recuperación ante incidentes de seguridad.

Asimismo, el desarrollo del laboratorio virtual facilita la comprensión de conceptos fundamentales como reconocimiento, escaneo de vulnerabilidades, explotación controlada, movimiento lateral, análisis forense, respuesta a incidentes y hardening de sistemas, permitiendo observar de manera práctica cómo una debilidad de seguridad puede afectar múltiples activos tecnológicos dentro de una infraestructura de red.

De igual forma, este trabajo contribuye a la formación ética y profesional del futuro ingeniero, al promover el análisis crítico de situaciones relacionadas con la legalidad de las actividades de ciberseguridad, la protección de datos, la responsabilidad profesional y el cumplimiento de marcos normativos y códigos de ética aplicables al ejercicio de la profesión.

Estos aspectos son esenciales para garantizar que el conocimiento técnico sea utilizado de manera responsable y en beneficio de la comunidad tecnológica.

Finalmente, la elaboración de este informe se justifica por la necesidad de integrar conocimientos técnicos, legales y organizacionales que permitan comprender la importancia de implementar controles de seguridad efectivos y fomentar una cultura de protección de la información, contribuyendo al fortalecimiento de las capacidades de ciberseguridad en las organizaciones actuales.

Objetivos

Objetivo General

Diseñar estrategias de mitigación, contención y respuesta a incidentes de seguridad informática mediante la identificación, explotación controlada y análisis de vulnerabilidades presentes en una infraestructura de TI simulada, integrando capacidades ofensivas de red team y defensivas de blue team para fortalecer la seguridad organizacional.

Objetivos Específicos

Identificar las vulnerabilidades presentes en la infraestructura TI mediante el análisis de servicios, sistemas operativos y procesos de red que puedan ser aprovechados por un atacante.

Analizar los riesgos asociados a amenazas internas y externas, evaluando por medio de procesos de red team el impacto que estas pueden generar sobre la disponibilidad, integridad y confidencialidad de la información.

Implementar estrategias de contención basadas en procesos de blue team para la detección, monitoreo y respuesta ante incidentes de seguridad informática.

Proponer mecanismos de fortalecimiento de la seguridad mediante controles de monitoreo, segmentación de red y medidas de mitigación orientadas a la protección de los activos tecnológicos.

Fundamentos de Operaciones red team y blue team

Legislación en Colombia sobre delitos informáticos y protección de datos personales

La transformación digital ha generado importantes beneficios para las organizaciones, las entidades gubernamentales y la sociedad en general. Sin embargo, el incremento en el uso de tecnologías de la información y las comunicaciones también ha propiciado el surgimiento de nuevas amenazas asociadas a la ciberdelincuencia, tales como el acceso no autorizado a sistemas informáticos, el robo de información, la interceptación de comunicaciones y la utilización indebida de datos personales.

Ante este panorama, Colombia ha desarrollado un marco normativo orientado a proteger tanto la información digital como los datos personales de los ciudadanos. Este conjunto de leyes y decretos establece responsabilidades para las organizaciones, reconoce derechos para los titulares de la información y define sanciones para quienes vulneren la seguridad de los sistemas informáticos. Entre las normas más relevantes se encuentran la Ley 1273 de 2009, la Ley 1581 de 2012 y varios decretos reglamentarios que complementan su aplicación práctica. (Guarnizo, 2024).

Ley 1273 de 2009: Protección Jurídica de la Información y los Datos

La Ley 1273 de 2009 representa uno de los principales avances de Colombia en materia de ciberseguridad. Esta norma modificó el Código Penal colombiano incorporando un nuevo bien jurídico denominado “Protección de la Información y de los Datos”, con el propósito de salvaguardar los sistemas informáticos y la información que se almacena, procesa o transmite mediante tecnologías digitales.

El principal objetivo de esta ley es garantizar la protección de los tres pilares fundamentales de la seguridad de la información:

Confidencialidad: asegurar que la información solo sea accesible para personas autorizadas.

Integridad: preservar la exactitud y consistencia de los datos, evitando modificaciones no autorizadas.

Disponibilidad: garantizar que la información y los sistemas estén accesibles cuando sean requeridos.

Para cumplir con este propósito, la ley tipifica diversos delitos informáticos, entre los que se destacan:

- Acceso abusivo a sistemas informáticos.
- Obstaculización ilegítima de sistemas o redes de telecomunicaciones.
- Interceptación de datos informáticos.
- Daño informático.
- Uso y propagación de software malicioso.
- Hurto por medios informáticos.
- Transferencia no consentida de activos.

Las personas que incurran en estas conductas pueden enfrentar sanciones que incluyen penas privativas de la libertad y multas económicas significativas, cuya gravedad dependerá de la magnitud del daño causado y de las circunstancias específicas del delito.

La importancia de esta ley radica en que proporciona herramientas legales para perseguir y sancionar los ataques cibernéticos que afectan tanto a ciudadanos como a organizaciones públicas y privadas.

En el caso de SecureNova Labs, la explotación del servicio HFS sobre Host A y el posterior movimiento lateral hacia Host B solo son jurídicamente válidos porque se ejecutan

dentro de un entorno controlado y con fines de evaluación de seguridad. Sin autorización formal, estas mismas acciones podrían constituir delitos informáticos sancionables penalmente.

Este aspecto también adquiere especial importancia frente al análisis ético del acuerdo de confidencialidad estudiado, ya que cualquier cláusula orientada a encubrir actividades ilegales o impedir la denuncia de delitos informáticos contraviene directamente la legislación colombiana. (*Cancillería | Ministerio de Relaciones Exteriores de Colombia*, 2018).

Ley 1581 de 2012: Régimen General de Protección de Datos Personales

La Ley 1581 de 2012 establece el marco general para la protección de los datos personales en Colombia. Su finalidad principal es garantizar que toda persona tenga control sobre la información que la identifica y que es recopilada, almacenada o utilizada por terceros.

Esta normativa reconoce el derecho de los ciudadanos a conocer, actualizar, rectificar y solicitar la eliminación de sus datos personales cuando corresponda. Asimismo, exige que las organizaciones implementen medidas que permitan un tratamiento responsable y seguro de la información.

La ley se fundamenta en varios principios esenciales:

Principio de legalidad

Todo tratamiento de datos debe realizarse conforme a las disposiciones legales vigentes.

Principio de finalidad

La recolección de datos debe responder a un propósito legítimo, específico y previamente informado al titular.

Principio de libertad

Los datos personales solo pueden ser tratados con autorización previa, expresa e informada del titular, salvo las excepciones establecidas por la ley.

Principio de veracidad

La información almacenada debe ser exacta, actualizada y verificable.

Principio de seguridad

Los responsables del tratamiento deben implementar controles técnicos, administrativos y físicos para proteger la información.

Principio de confidencialidad

Las personas que intervienen en el tratamiento de datos están obligadas a mantener reserva sobre la información a la que tengan acceso.

Entre los derechos que esta ley otorga a los titulares de los datos se encuentran:

- Conocer la información almacenada sobre ellos.
- Solicitar correcciones o actualizaciones.
- Presentar consultas y reclamos.
- Solicitar la eliminación de datos cuando sea procedente.
- Revocar la autorización otorgada para el tratamiento de la información.

La norma aplica tanto para entidades públicas como privadas que recolecten o administren datos personales dentro del territorio colombiano. (*Ley 1581 de 2012 - Gestor Normativo*, 2023).

En el caso de SecureNova Labs, la explotación de sistemas comprometidos podría exponer información sensible como credenciales, direcciones IP, configuraciones internas, registros de eventos, archivos corporativos o datos personales de usuarios. Bajo esta normativa, cualquier tratamiento de dicha información debe cumplir principios fundamentales como legalidad, finalidad, libertad, seguridad y confidencialidad.

Desde la perspectiva red team, esto implica que los profesionales deben limitar el alcance de sus pruebas exclusivamente a los activos autorizados y evitar cualquier recolección innecesaria de información personal. Desde la perspectiva blue team, implica la obligación de

proteger adecuadamente los datos comprometidos durante el incidente, evitando exposición adicional, fugas de información o accesos no autorizados durante las actividades de análisis y respuesta.

Por tanto, la gestión de incidentes en SecureNova Labs no solo debe enfocarse en contener el ataque, sino también en proteger los datos personales potencialmente expuestos durante la intrusión.

Decreto 1377 de 2013: Reglamentación de la Protección de Datos Personales

El Decreto 1377 de 2013 fue expedido con el propósito de desarrollar y reglamentar varios aspectos contemplados en la Ley 1581 de 2012, proporcionando directrices más específicas para las organizaciones que realizan tratamiento de datos personales.

Uno de los aspectos más importantes del decreto es la regulación de la autorización del titular. Como regla general, ninguna organización puede recolectar o utilizar datos personales sin haber obtenido previamente el consentimiento del titular.

Adicionalmente, el decreto introduce la figura del Aviso de Privacidad, mediante el cual las organizaciones deben informar a los ciudadanos sobre:

- La existencia de políticas de tratamiento de datos.
- Las finalidades para las cuales se recopila la información.
- Los mecanismos disponibles para ejercer sus derechos.

De igual forma, obliga a las entidades a elaborar y mantener actualizadas políticas de tratamiento de datos personales, garantizando que estas sean accesibles para los titulares y que se cumplan de manera efectiva.

Gracias a esta reglamentación, las disposiciones generales de la Ley 1581 adquirieron una aplicación práctica más clara y uniforme. (*Decreto 1377 de 2013 - Gestor Normativo*, 2015).

Decreto 886 de 2014: Registro Nacional de Bases de Datos

Con el fin de fortalecer la supervisión y el control sobre el tratamiento de datos personales, el Decreto 886 de 2014 reglamentó el Registro Nacional de Bases de Datos (RNBD), creado por la Ley 1581 de 2012.

Este registro constituye una herramienta administrada por la Superintendencia de Industria y Comercio (SIC), mediante la cual las organizaciones deben reportar información relacionada con las bases de datos que administran.

Entre los elementos mínimos que deben registrarse se encuentran:

- Identificación del responsable del tratamiento.
- Información de contacto.
- Identificación de los encargados del tratamiento.
- Finalidad de la base de datos.
- Forma de almacenamiento y tratamiento.
- Políticas de protección de datos implementadas.
- Canales habilitados para la atención de consultas y reclamos.

La creación del RNBD busca aumentar la transparencia en el manejo de la información personal y facilitar el ejercicio de los derechos de los titulares. (*Decreto 886 de 2014 - Gestor Normativo*, 2015).

Decreto Único Reglamentario 1074 de 2015

El Decreto 1074 de 2015 consolidó en un único cuerpo normativo diversas disposiciones reglamentarias relacionadas con el sector Comercio, Industria y Turismo, incluyendo aquellas referentes a la protección de datos personales.

Aunque su alcance es amplio, este decreto resulta especialmente importante porque integra y organiza las obligaciones administrativas relacionadas con el tratamiento de datos personales, facilitando su consulta y aplicación por parte de las organizaciones.

Asimismo, establece lineamientos operativos para el cumplimiento de las disposiciones legales y fortalece las facultades de vigilancia y control de la Superintendencia de Industria y Comercio. (*Decreto 1074 de 2015 Sector Comercio, Industria Y Turismo - Gestor Normativo*, 2025).

Importancia de los Decretos Reglamentarios

Los decretos que complementan la legislación sobre protección de datos cumplen una función fundamental dentro del sistema jurídico colombiano. Mientras las leyes establecen principios generales y derechos, los decretos determinan la manera práctica en que dichos principios deben implementarse.

- En términos generales, estos decretos:
- Definen procedimientos y obligaciones específicas para las organizaciones.
- Establecen mecanismos de control y supervisión.
- Facilitan el cumplimiento normativo.
- Promueven mejores prácticas en el manejo de la información.
- Fortalecen las capacidades de inspección, vigilancia y sanción de la Superintendencia de Industria y Comercio.

En conclusión, la legislación colombiana en materia de delitos informáticos y protección de datos personales constituye un marco normativo integral que busca responder a los desafíos de la transformación digital y al crecimiento de las amenazas cibernéticas. Mientras la Ley 1273 de 2009 se enfoca en la prevención y sanción de conductas que afectan la seguridad de los

sistemas informáticos, la Ley 1581 de 2012 y sus decretos reglamentarios garantizan la protección de los datos personales y el respeto por los derechos de los ciudadanos.

El cumplimiento de estas disposiciones no solo representa una obligación legal para las organizaciones, sino también una estrategia fundamental para fortalecer la confianza de los usuarios, proteger los activos de información y contribuir al desarrollo de una cultura de seguridad digital en Colombia.

En el escenario de SecureNova Labs, estas disposiciones tienen implicaciones directas en varios aspectos críticos:

Autorización de pruebas de seguridad: Toda actividad de pentesting debe estar respaldada por documentos formales que definan alcance, objetivos, activos autorizados, reglas de enfrentamiento y responsabilidades legales. Esto evita que una actividad legítima de red team pueda interpretarse como una intrusión ilegal.

Tratamiento de datos recolectados: Durante ejercicios ofensivos y defensivos se generan evidencias como capturas de tráfico, logs, credenciales, hashes, volcados de memoria y registros de acceso. Esta información debe almacenarse, protegerse y tratarse bajo estrictos controles de confidencialidad.

Preservación de evidencia digital: Desde el enfoque blue team, la preservación de evidencia resulta crítica para análisis forense, auditorías internas o eventuales procesos judiciales. Logs del SIEM, registros de firewall, trazas de red y evidencias de sesiones Meterpreter deben conservarse garantizando integridad, trazabilidad y cadena de custodia.

Reporte de incidentes y denuncia de irregularidades: Las organizaciones deben contar con procedimientos formales para reporte, escalamiento y gestión de incidentes. En el caso de detectar accesos indebidos, espionaje o actividades ilícitas, no solo existe una obligación técnica

de respuesta, sino también responsabilidad legal y ética de denunciar irregularidades cuando corresponda.

Límites éticos y responsabilidad profesional en ciberseguridad: El caso de SecureNova Labs también evidencia que la ciberseguridad no depende únicamente del dominio técnico de herramientas ofensivas y defensivas. El profesional debe actuar bajo principios éticos, legales y de responsabilidad social. (Ministerio de Tecnologías de la Información y las Comunicaciones - *2020 Secciones*, 2020).

Etapas del pentesting y herramientas utilizadas en cada una de ellas

El pentesting o pruebas de penetración en términos simples, consiste en realizar ataques controlados a las redes y sistemas de una organización con el fin de encontrar vulnerabilidades y poder gestionarlas para evitar la materialización de ataques externos. Puede realizarse pentesting de caja blanca (cuando se conoce la infraestructura a evaluar, lo que permite más profundidad en las pruebas pero le resta realismo), de caja negra (cuando no se conoce la infraestructura a evaluar, lo que le aporta más realismo) y de caja gris (donde se tiene un conocimiento parcial de la infraestructura a evaluar y es posible conseguir un equilibrio entre la profundidad del de caja blanca y el realismo del de caja negra) (Chindruş & Căruntu, 2023) .

Etapas:

- **Reconocimiento:** Es la fase inicial del pentesting y de un buen reconocimiento depende el éxito del proceso en general porque en este se determinan los sistemas, servicios o aplicaciones a evaluar. Herramientas como Nmap son utilizadas en esta fase del proceso.
- **Escaneo de vulnerabilidades:** Por medio de herramientas avanzadas para la identificación de vulnerabilidades como OpenVAS, Nessus, Acunetix, SQLMap, entre

otras; se realizan búsquedas de configuraciones, versiones de los sistemas operativos y servicios en uso para identificar posibilidades de ataque. Existen herramientas especializadas que permiten realizar este proceso de manera automática y que facilitan mucho el proceso porque realizarlo de manera manual implica consumo excesivo de tiempo y aumenta el riesgo de errores humanos.

- **Explotación:** Identificados los sistemas e infraestructuras, además de sus vulnerabilidades; esta etapa consiste en realizar ataques por medio de herramientas como Metasploit Framework, Hydra, Aircarck-ng, entre otras; para poner a prueba dichas vulnerabilidades y determinar si representan una amenaza real y son explotables. Para el caso de que sean explotables es muy importante determinar el impacto de la materialización de un ataque y el compromiso para la organización y sus activos de información.
- **Post-Explotación:** Es muy importante esta fase porque en ella se identifican servicios ocultos que también pueden ser explotables y evaluar el impacto para la organización. Herramientas como GhostPack y Cobalt Strike son usuales en esta etapa del proceso.
    - **Informe y Mitigación:** Es la fase final del proceso y consiste en recopilar por medio de un informe, las vulnerabilidades encontradas y se detalla el proceso realizado con ellas, además se define los procesos necesarios para la mitigación de las vulnerabilidades. Para esta fase suelen utilizarse herramientas como Dradis Framework, SysReptor, PwnDoc, entre otras; que permiten centralizar los avances del equipo a cargo del pentesting y luego exportarlos en formatos usuales como PDF o Word con el fin de hacerlos entendibles para todos. (Lozano, 2023) .

Herramientas de ciberseguridad utilizadas para ejercicios de pentesting

- Metasploit: Es una herramienta de código abierta ampliamente utilizada para pruebas de penetración (pentesting) y hacking ético, es de gran utilidad para la explotación y valoración de vulnerabilidades de seguridad en sistemas informáticos. Sus principales funciones son: escaneo, detección y explotación de vulnerabilidades, evasión de seguridad, automatización de auditorías; su gran versatilidad en diferentes escenarios la hace ideal para ejercicios de red team y blue team
- Nmap: Es una herramienta de código abierto utilizada para auditorías de seguridad y administración de redes, permite la visualización de equipos, mapeo de redes, detección de puertos abiertos, identificación de servicios y aplicaciones así como sus versiones y vulnerabilidades.
- OpenVas: Es una herramienta de código abierto ampliamente utilizada porque es un poderoso escáner de vulnerabilidades que permite identificar, analizar y gestionar fallos de seguridad en equipos, redes e infraestructuras informáticas

Servicios en línea:

- ExploitDB: Es una base de datos gratuita y abierta que es utilizada como importante herramienta por profesionales en ciberseguridad porque contiene un amplio repositorio de vulnerabilidades, exploits y códigos de prueba que son insumos indispensables en la realización de pentesting.
- CVE: Es un sistema estandarizado que sirve para identificar, catalogar y anunciar las vulnerabilidades de seguridad conocidas, para software y hardware. Por medio de este sistema se proporciona un ID único que permite codificar cada fallo, lo que permite a las organizaciones la fácil identificación, priorización y aplicación de parches de seguridad

para las vulnerabilidades encontradas. (*¿Qué Es El Pentesting? Auditando La Seguridad de Tus Sistemas | Empresas | Instituto Nacional de Ciberseguridad |INCIBE*, 2021).

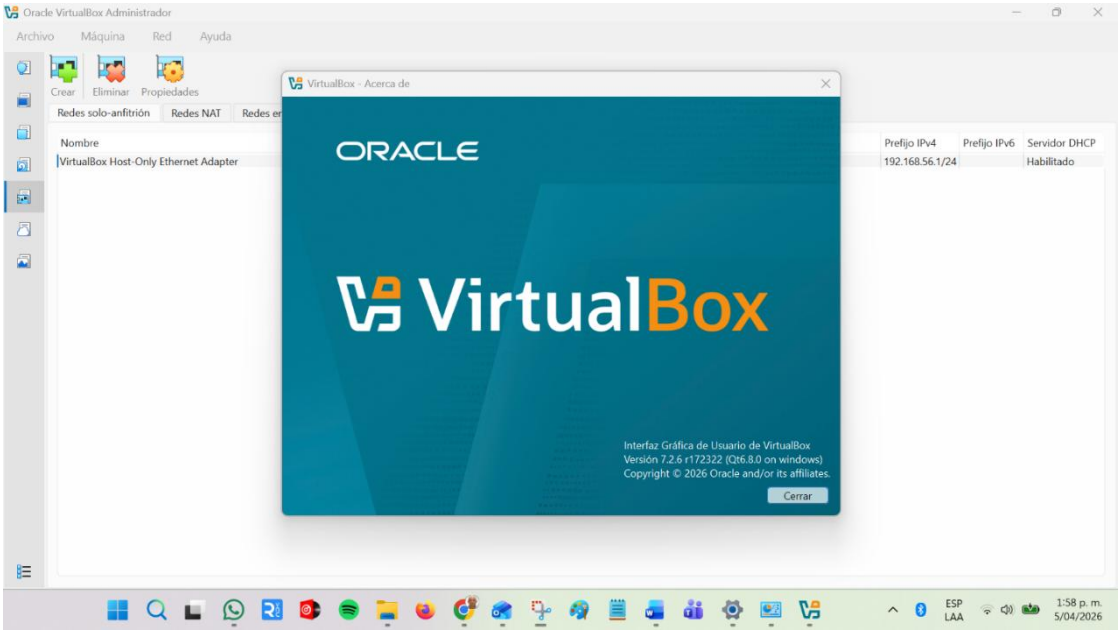
Implementación del laboratorio virtual para pruebas de pentesting

Paso A: Descargar la herramienta de virtualización VirtualBox en su última versión.

Paso B: Ingresar al link entregado para la descarga de los insumos que serán utilizados en la realización del laboratorio propuesto.

El enlace conduce a la página web para descarga del software de virtualización VirtualBox por medio del cual pueden realizarse ejercicios de simulación con máquinas virtuales que funcionan igual que una máquina física y permiten la realización de cualquier operación que implique la utilización de redes informáticas (*Oracle VirtualBox*, 2026).

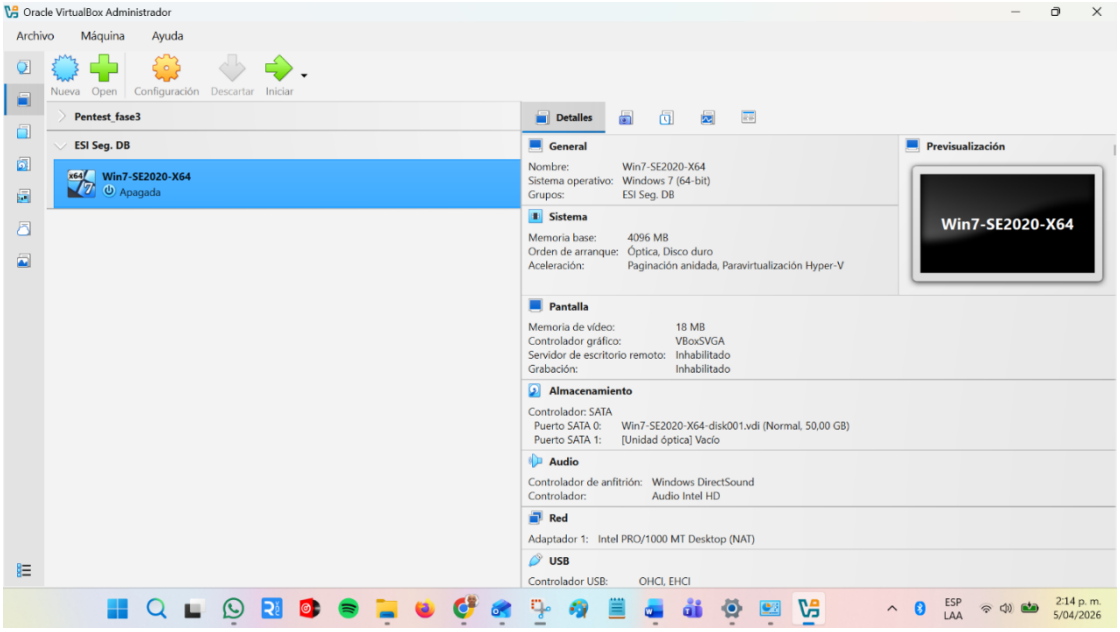
Figura 1
Instalación VirtualBox versión 7.2.6



Nota. Evidencia de instalación de la versión más reciente del software para virtualización VirtualBox, la figura es de autoría del propio autor.

Los virtualizadores, como Oracle VM VirtualBox, son herramientas de software que permiten crear y ejecutar máquinas virtuales dentro de un computador físico. Su función principal es simular el hardware de un equipo independiente, posibilitando la instalación y uso de diferentes sistemas operativos (como Kali Linux, Windows o Ubuntu) sin necesidad de modificar el sistema operativo principal. Estos entornos son ampliamente utilizados para pruebas de software, laboratorios de ciberseguridad, desarrollo, capacitación y análisis de sistemas, ya que permiten experimentar de forma segura, aislada y controlada, reduciendo riesgos sobre el equipo anfitrión.

Figura 2
Instalación máquina virtual Windows



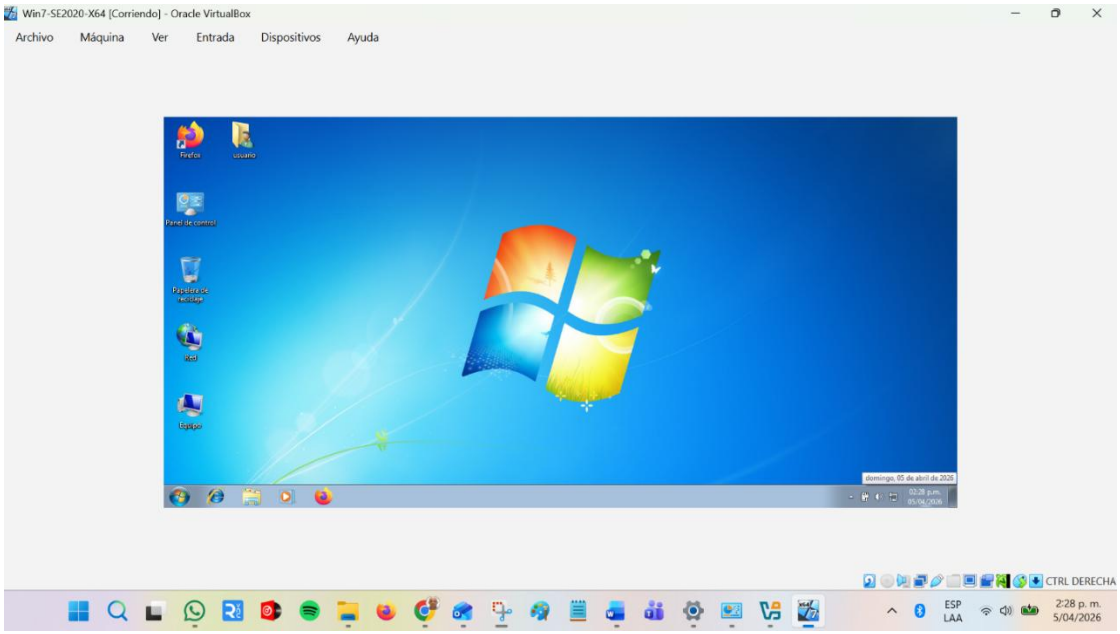
Nota. Instalación en VirtualBox de una máquina virtual Windows 7 para realización de ejercicio de pentesting, la figura es de autoría del propio autor.

Con la imagen ISO de la máquina virtual (que para el caso puntual es una máquina Windows 7 es entregada dentro de los insumos iniciales) se procede a realizar la instalación en la herramienta de virtualización de la máquina virtual que será utilizada para la realización del

ejercicio de pentesting y se asignan los recursos necesarios de acuerdo con las capacidades de la máquina física (RAM, procesamiento, condiciones de red, etc.) para garantizar que las máquinas requeridas puedan operarse y lograr la conectividad entre ellas permitiendo la realización de cada uno de los pasos propuestos para evidenciar la manera en que una vulnerabilidad existente en uno de los equipos de una red, puede explotarse y alcanzar otros dispositivos para la obtención de control y privilegios de administración que le entregan al atacante lo necesario para sustraer información, cifrar datos y en general para comprometer los sistemas informáticos de una organización.

Figura 3

Máquina virtual Windows corriendo



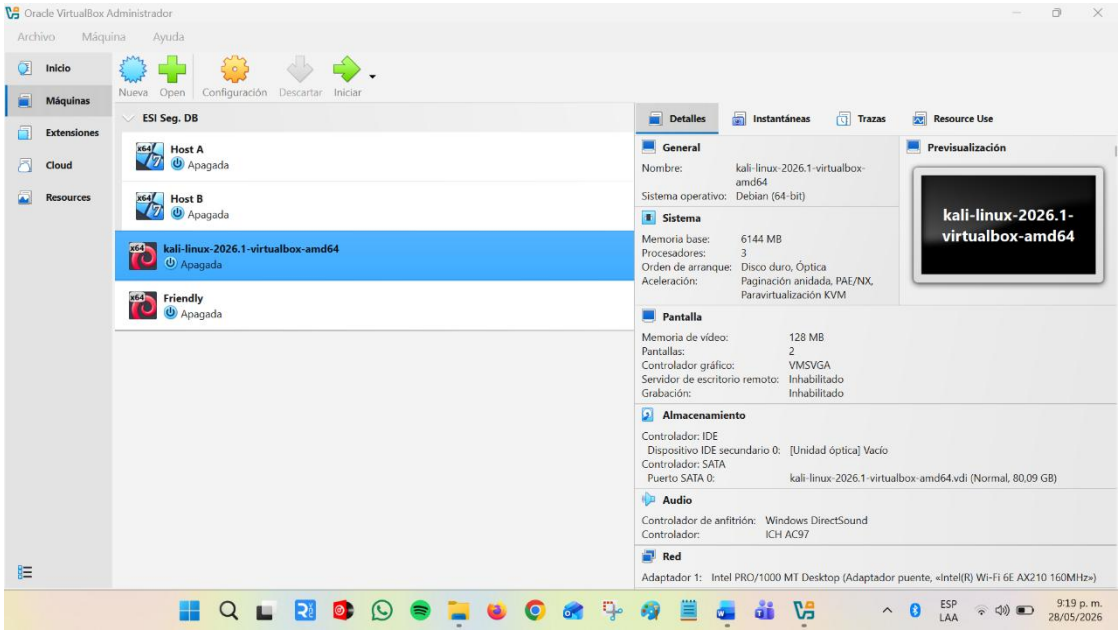
Nota. Evidencia de la operación en VirtualBox de la máquina virtual Windows 7 instalada, la figura es de autoría del propio autor.

En la imagen se observa la máquina virtual Windows 7 llamada Host A funcionando de manera virtual, después de realizado el proceso de instalación y asignación de recursos de la máquina física. En este momento puede realizarse cualquier acción como si se tratara de una máquina física; puede instalarse software, cargar y descargar archivos, crear y eliminar usuarios,

modificar características de funcionamiento, etc., para el ejercicio propuesto se debe infectar la máquina con un archivo HFS, lo cual consiste en simplemente por una capeta compartida llevar al escritorio de dicho equipo un ejecutable que aunque no se observe en funcionamiento, sí permite que el atacante (en este caso el especialista del equipo red team) pueda acceder y explotar las vulnerabilidades que le aporta el hecho de contar con el ejecutable en mención.

Figura 4

Instalación máquina virtual Kali Linux



Nota. Instalación en VirtualBox de la máquina virtual Kali Linux para realización de ejercicio de pentesting, la figura es de autoría del propio autor.

Al igual que con la máquina Windows 7, debe contarse con la imagen ISO para el proceso de instalación de la máquina virtual Kali Linux que en este caso será utilizada para la realización del proceso de pentesting. Durante una prueba de pentesting en un entorno virtualizado con VirtualBox, se configura inicialmente una máquina atacante con Kali Linux y una máquina objetivo con Windows (Host A) dentro de una misma red virtual para garantizar la conectividad controlada entre ambas. El proceso inicia con la fase de reconocimiento, en la cual

se identifican direcciones IP, puertos abiertos y servicios activos en la máquina Windows mediante herramientas de escaneo y enumeración. Posteriormente, se realiza el análisis de vulnerabilidades para detectar posibles debilidades en el sistema objetivo. Con base en los hallazgos, se ejecuta la fase de explotación, buscando validar si las vulnerabilidades identificadas pueden ser aprovechadas para obtener acceso no autorizado o elevar privilegios.

Figura 5
Máquina virtual Kali Linux corriendo

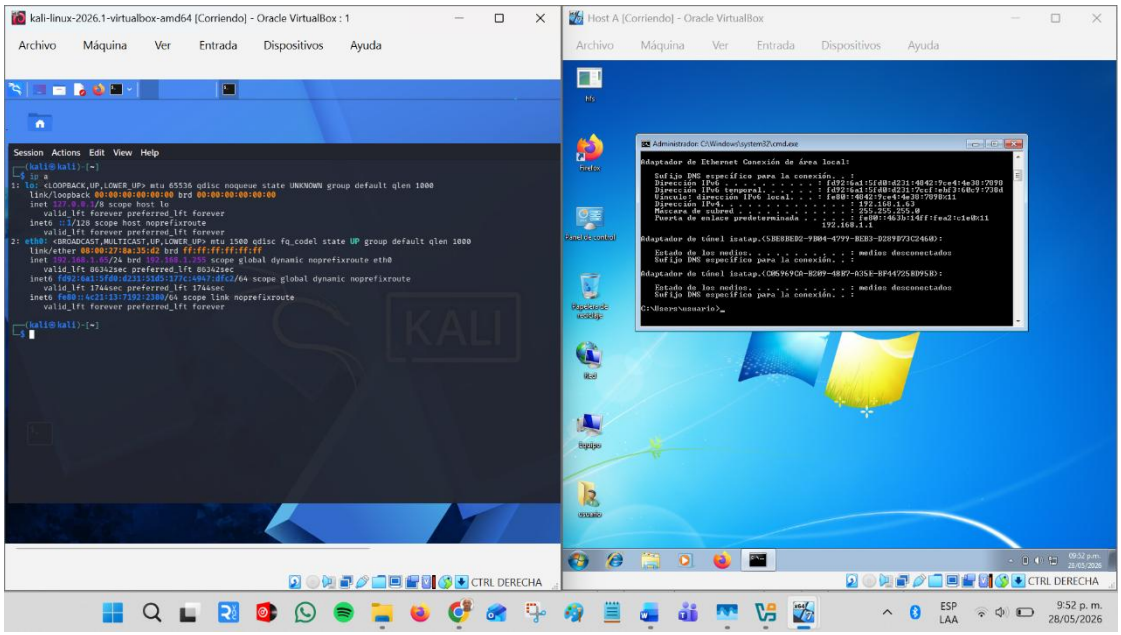
Nota. Evidencia de la operación en VirtualBox de la máquina virtual Kali Linux instalada, la figura es de autoría del propio autor.

En la imagen se observa la máquina virtual Kali Linux corriendo esta no es otra cosa que un entorno aislado diseñado principalmente para tareas de ciberseguridad, análisis forense, pruebas de penetración y evaluación de vulnerabilidades. Kali Linux incorpora una amplia variedad de herramientas especializadas para auditorías de seguridad, análisis de redes, explotación de vulnerabilidades y pruebas de seguridad ofensiva. Su implementación dentro de VirtualBox permite trabajar en un entorno controlado y seguro, sin afectar el sistema operativo

físico, facilitando la creación de laboratorios virtuales para simulaciones, prácticas académicas y pruebas técnicas en escenarios reales o controlados. Dentro del amplio abanico de posibilidades que ofrece este tipo de entorno se encuentra la articulación con poderosas herramientas desarrolladas especialmente para procesos propios de los procesos de pentesting y que incluso algunas pueden utilizarse en varias etapas.

Figura 6

Verificación de IPs para Kali Linux y Host A



Nota. Verificación en VirtualBox mediante consola de comandos de las IPs por defecto de las máquinas virtuales Kali Linux y Windows 7 instaladas, la figura es de autoría del propio autor.

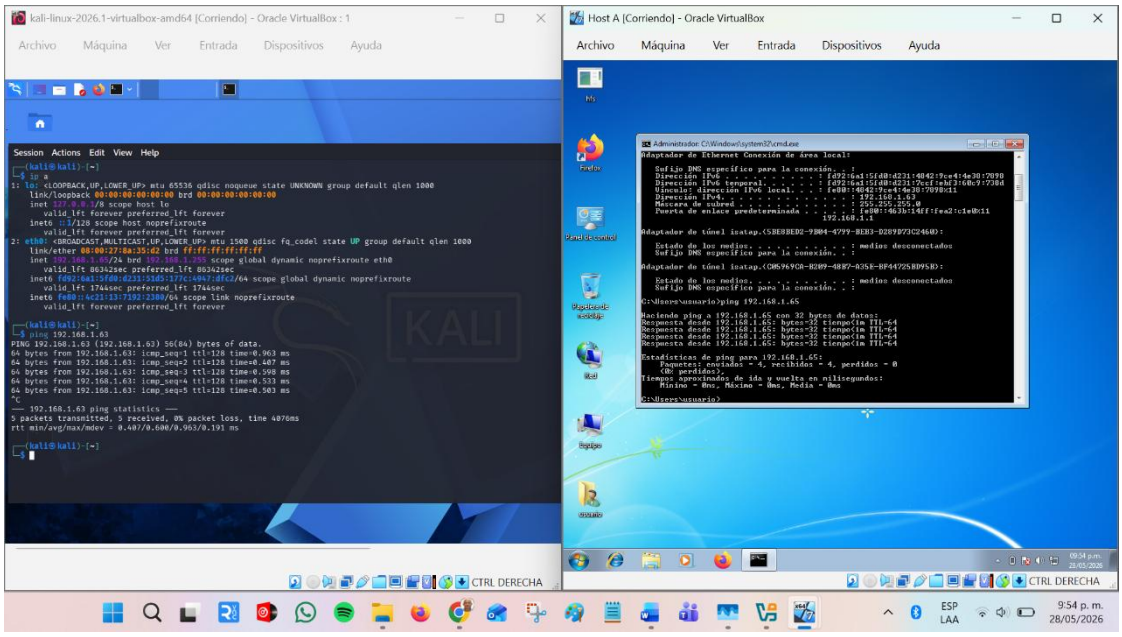
Lo primero para garantizar que las máquinas virtuales establezcan comunicación es configurar sus respectivos adaptadores de red para conectar a “Adaptador puente”, con esto se logra que por DHCP cada máquina virtual tome por defecto una dirección IP dentro del mismo segmento, además que al identificarlas por consola de comandos y enviar ping desde y hacia cualquiera de las dos; estos respondan permitiendo establecer la primera condición importante

para garantizar que el proceso de pentesting sea exitoso, pues si la máquina Kali Linux no puede alcanzar la IP del Host A, resulta improbable que pueda acceder y atacarlo.

Paso C: Verificar que exista comunicación entre las máquinas *Windows* y la máquina *Kali Linux*. Tener en cuenta que no deben encenderse ambas máquinas virtuales al mismo tiempo, ya que esto puede afectar los recursos de hardware del equipo host. Encender primero una máquina Windows y posteriormente la máquina Kali Linux.

Figura 7

Pruebas de conectividad entre Kali Linux y Host A por medio de ping



Nota. Verificación en VirtualBox mediante consola de comandos de conectividad por medio de ping entre las máquinas virtuales Kali Linux y Windows 7 instaladas, la figura es de autoría del propio autor.

En la imagen se observan las consolas de comandos desplegadas tanto en la máquina Kali Linux como en el Host A y en cada una de ellas puede evidenciarse la IP que tiene configurada, además de la respuesta al ping enviado en ambas direcciones.

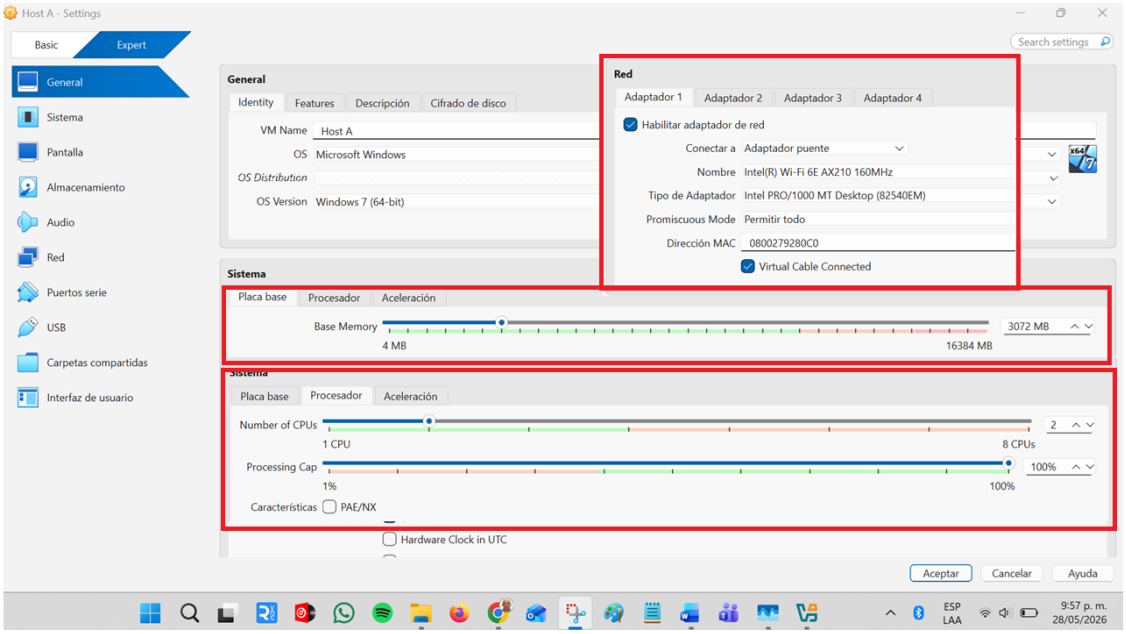
Paso D: Evidencia mediante capturas de pantalla del montaje del laboratorio y explicación de cómo se encuentra desplegado, incluyendo las características técnicas de hardware asignadas.

En cada máquina virtual se asignan capacidades del sistema como memoria RAM, procesadores y configuraciones de red; de acuerdo con los recursos existentes en la máquina física.

A continuación, por medio de capturas de pantalla se evidencian las capacidades operacionales asignadas a cada una de las máquinas virtuales y las configuraciones simples que permiten la conectividad entre las mismas sin crear una red local específica, procedimiento que pudo evidenciarse en la Figura 7 con la verificación de la IP tomada de manera automática por cada una de las máquinas virtuales y la verificación de respuesta de ping entre ambas.

Figura 8

Configuraciones para Host A en VirtualBox



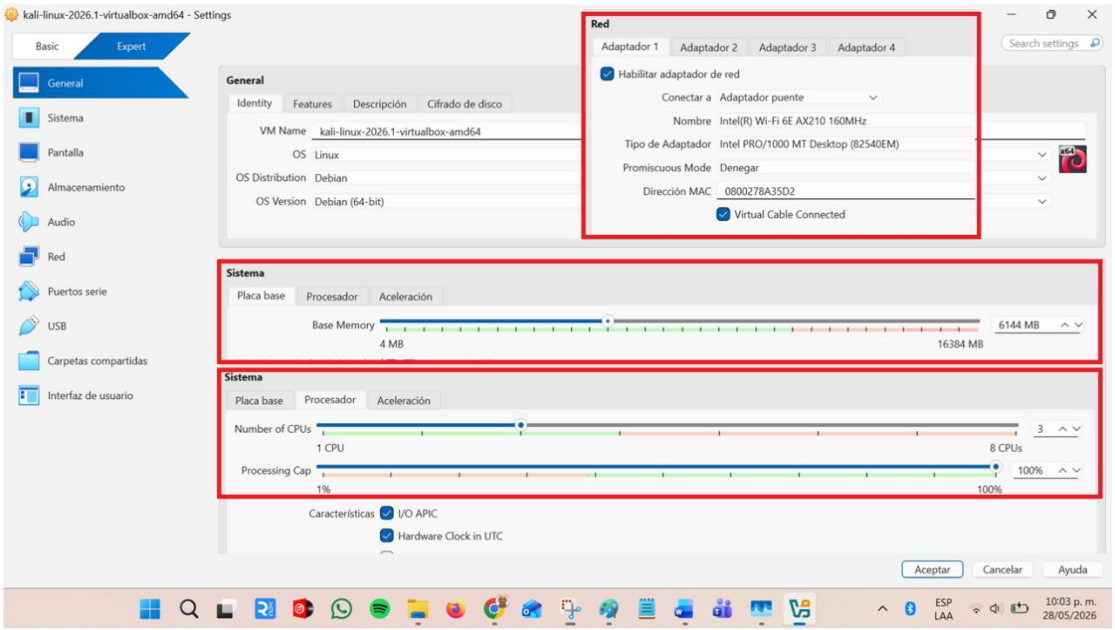
Nota. Evidencia de la configuración de red y asignación de recursos en VirtualBox para la máquina virtual Windows 7, la figura es de autoría del propio autor.

Considerando las capacidades de la máquina física se asignan los recursos que garanticen que la máquina virtual pueda operar y permitir la realización de las pruebas establecidas sin afectar la

operación de las demás máquinas virtuales que componen el laboratorio y de la máquina anfitriona que finalmente es la que debe funcionar de mejor manera para llevar a buen término las pruebas propuestas. Para el caso del Host A se deben configurar dos adaptadores de red: uno como adaptador puente (para conectarse a la misma red de la máquina Kali Linux) y el otro como red NAT (que funciona como una red LAN) en un segmento fijo dende también se encontrará el Host B.

Figura 9

Configuraciones para Kali Linux en VirtualBox



Nota. Evidencia de la configuración de red y asignación de recursos en VirtualBox para la máquina virtual Kali Linux, la figura es de autoría del propio autor.

Como se observa en las Figuras 8 y 9, es necesario asignar capacidades reales de la máquina física a las máquinas virtuales; tanto el Host A como la máquina Kali Linux deben contar con los recursos mínimos necesarios para garantizar su operación, siempre garantizando que no se superen las capacidades reales de la máquina física. En el caso de la máquina Kali Linux se asignan mejores capacidades para garantizar un mejor funcionamiento considerando

que esta será la máquina desde la que se realizarán todos y cada uno de los pasos del ejercicio de pentesting propuesto. (Trigos, 2026) (*Pentesting | Instituto Nacional de Ciberseguridad | INCIBE*, 2021).

Análisis ético y legal del acuerdo de confidencialidad

Para el desarrollo de estos aspectos se propone la lectura y análisis de los documentos Anexo 2 – escenario 2 y Anexo 3 – Acuerdo, para contextualizar los siguientes aspectos, argumentando y señalando los fragmentos del anexo en caso de existir alguna irregularidad:

Evidencias de procesos ilegales y no éticos que se esté estipulando en dicho acuerdo:

Revisando el contenido del Anexo 3 – Acuerdo y contrastándolo con las leyes colombianas y con principios éticos mínimos que deberían hacer parte de un profesional integral, surgen las siguientes situaciones que no pueden ser aceptables para el desarrollo de una actividad laboral en las condiciones justas mínimas para la "parte receptora" establecida en el acuerdo:

Contexto que alerta sobre los riesgos de posibles irregularidades

En el Anexo 2 – Escenario 2 se advierte explícitamente que: "El contrato y el acuerdo de confidencialidad… fueron elaborados por un abogado que ya no labora en la organización… tras detectarse posibles irregularidades en su gestión… lo cual genera riesgos de incluir cláusulas con procesos ilícitos o contrarios a la ética profesional"

De entrada esto establece una alerta jurídica, al indicar que los documentos requeridos para la firma inicial del contrato laboral (contrato y acuerdo) pueden contener disposiciones inválidas o ilegales.

Cláusulas que evidencian la realización de procesos ilegales

A. Encubrimiento de actividades ilegales

En la Cláusula Primera. Objeto: Se establece:

"…la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados."

Irregularidad: Prohibir a la parte receptora la divulgación de actividades ilegales que pueda encontrarse en el cumplimiento de sus labores, lo cual es arbitrario y totalmente contrario a la ley porque nadie puede obligar a otra persona a guardar silencio sobre la comisión de delitos. Se falta a principios legales básicos como:

Deber de denuncia

Preservación del interés público

Actuar dentro de las normas penales (en Colombia, encubrimiento u omisión de denuncia).

B. Reconocimiento explícito de actividades ilícitas

En la Cláusula Segunda: Definición de información confidencial: Donde se enumera lo que para la organización es considerado "Información Confidencial" se intentan camuflar actividades delictivas dentro de actividades que pueden ser legales y hacer parte de las actividades de la organización, que al ser clasificados como información confidencial; terminan normalizando la comisión de delitos: "…datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

Irregularidad: La cláusula menciona expresa y directamente delitos informáticos, algunos tipificados en leyes colombianas:

Interceptación ilegal (Ley 1273 de 2009 en Colombia)

Acceso abusivo a sistemas

Esto no solo es faltar ante la ética profesional del aspirante, sino que al aceptar esta cláusula estaría incurriendo en delitos como: Concierto para delinquir y uso indebido de información, en la realización de actividades ajenas a su responsabilidad.

C. Prohibición para denunciar delitos

En la Cláusula Cuarta: Obligaciones de la parte receptora: Se inicia con un enunciado que se presta para interpretar que esta puede ser modificada a conveniencia de la organización, en el momento que esta lo considere: “De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes”, además en los numerales 3 y 4: “No denunciar ante las autoridades actividades sospechosas de espionaje…” y “Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca…” se obliga a la parte receptora a cometer acciones en contra de la ley

Irregularidad: Con la aceptación del acuerdo, la parte receptora se obliga explícitamente a:

No denunciar delitos

Ocultar información ilegal

Lo cual es ilegal (porque ningún contrato puede anular la obligación de denunciar delitos), nulo de pleno derecho (actos que por contradecir normas imperativas, son considerados totalmente ineficaces) y potencialmente constitutivo de delito.

D. Traslado indebido de responsabilidad penal

En el numeral 8 de la Cláusula Cuarta: se menciona que la parte receptora debe “Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento”

Irregularidad: Esto es completamente contrario a la ley porque quien debe responder por las actividades ilícitas que se encuentren realizando sus empleados en cumplimiento de sus funciones laborales, es la organización y no el empleado, a no ser que a este pueda probársele que las realizaba a título y/o beneficio propio y que la organización no tenía conocimiento. Esta situación también se evidencia en la Cláusula Octava donde se establece: “En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs”

lo cual es irregular porque pretende que el receptor asuma toda la responsabilidad e intenta eximir a la empresa de responsabilidad penal; esto es jurídicamente inválido porque la responsabilidad penal es personal e intransferible y esta no puede eliminarse mediante contratos privados.

E. Errores en la redacción del documento

Es evidente que el documento tiene graves fallas de redacción y orden en los procesos porque de la Cláusula Sexta pasa a la Cláusula Octava sin que pueda establecerse la razón de este error.

Irregularidad: Considerando la forma de actuar de la organización y que una cláusula anterior establece que "De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes" no se considera conveniente la aceptación de un documento que puede ser sujeto a cambios sin previo conocimiento de la parte receptora.

Conclusión: El acuerdo además de ilegal, es profundamente antiético porque fomenta el encubrimiento de delitos, obliga al profesional a actuar en contra de la ley y la ética profesional en ciberseguridad, normaliza prácticas como el espionaje ilegal, la interceptación de comunicaciones y los accesos indebidos; lo que en el contexto de red team / blue team, es especialmente grave porque estas actividades deben realizarse solo bajo autorización legal y en el acuerdo se sugiere un uso real y no controlado de técnicas ilícitas.

En consecuencia, el acuerdo no debería firmarse porque:

Las cláusulas serían nulas en un proceso legal y representa un riesgo jurídico alto para el firmante como receptor.

Vulneraciones a artículos de la ley 1273 existentes en el acuerdo de confidencialidad:

A continuación se realiza el análisis de cuáles artículos aplican y por qué se vulneran, relacionándolos directamente con el contenido del Anexo 3 - Acuerdo:

A. Acceso abusivo a un sistema informático (Artículo 269A)

Qué establece la ley 1273: Sanciona a quien acceda sin autorización a un sistema informático.

Evidencia en el acuerdo: "…datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"".

Por qué se vulnera la ley 1273: El acuerdo reconoce esta práctica como "información confidencial", no solo la menciona; sino que la normaliza dentro de la organización lo cual implica tolerancia ante este tipo de conducta o posible participación en accesos ilegales, lo cual es un delito.

B. Interceptación de datos informáticos (Artículo 269C)

Qué establece la ley 1273: Prohíbe interceptar datos sin orden judicial o autorización legítima.

Evidencia en el acuerdo: "…datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"".

Por qué se vulnera la ley 1273: El término "chuzadas" hace referencia directa a interceptaciones ilegales de comunicaciones, el acuerdo pretende proteger esta información dándole el estatus de información confidencial en lugar de denunciar; lo cual es un ilegal porque se configura el delito de interceptación ilegal.

C. Uso de software malicioso (Artículo 269E)

Qué establece la ley 1273: Sanciona la creación o uso de herramientas para vulnerar sistemas.

Relación con el acuerdo: Aunque no se menciona explícitamente software, el contexto de: accesos abusivos, espionaje e interceptación de información; implica el posible uso de herramientas ofensivas.

Por qué se vulnera la ley 1273: Estas actividades suelen requerir malware o herramientas de intrusión y el acuerdo no prohíbe estas prácticas, sino que tiende a encubrirlas.

D. Violación de datos personales (Artículo 269F)

Qué establece la ley1273: Sanciona el uso indebido de datos personales.

Evidencia en el acuerdo: Manejo de información sensible llamándola “información confidencial” obtenida por medio de interceptación de datos y espionaje.

Por qué se vulnera la ley 1273: Se accede y manipula información sin autorización además de no existir garantías de protección de datos, lo cual vulnera derechos fundamentales como: Habeas Data y Privacidad.

E. Transferencia no consentida de activos (Artículo 269J)

Qué establece la ley 1273: Castiga la manipulación de datos o sistemas para beneficio indebido.

Relación con el acuerdo: Incluye dentro de la información confidencial el acceso a información estratégica y el uso indebido de datos corporativos o de terceros.

Por qué se vulnera la ley 1273: El acceso ilegal a sistemas informáticos puede derivar en robo de información y manipulación de datos.

6. Relación clave: Encubrimiento de delitos

Qué establece la ley 1273: Aunque la Ley 1273 se enfoca en delitos informáticos, el acuerdo incluye algo aún más grave:

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

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

Por qué se vulnera la ley 1273: Porque esto implica encubrimiento de delitos informáticos y posible responsabilidad penal adicional (Código Penal Colombiano)

En síntesis: El acuerdo no solo es antiético, sino que podría involucrar directamente al firmante como parte receptora en delitos informáticos tipificados en la Ley 1273, generando responsabilidad penal y disciplinaria.

Conveniencia de aplicar a la oportunidad ofrecida por SecureNova Labs para experto en seguridad ante una buena oferta económica, condiciones laborales muy atractivas y la existencia de procesos poco confiables en la organización. Argumentación basada en lo dispuesto por COPNIA en su código de ética para ingenieros.

Personalmente declinaría mi intención de aplicar a la vacante ofertada debido a que por más favorables que sean las condiciones económicas y de estabilidad laboral que la organización pueda estar ofreciendo, se asume un alto riesgo de perder la tarjeta profesional al faltar al código de ética y siempre estará latente la posibilidad de verse inmerso en procesos con responsabilidad penal y/o legal, en los cuales puede suceder que el dinero recibido jamás compense los daños ocasionados con la comisión de delitos. Analizando las conductas en que podría incurrirse y contrastando con el código de ética de la entidad que regula la profesión, se realiza el siguiente análisis:

De acuerdo con el Código de Ética del Consejo Profesional Nacional de Ingeniería (COPNIA), un profesional que acepte firmar el acuerdo explicado en el Anexo 3 podría verse seriamente afectado tanto disciplinaria como legalmente, por las siguientes razones:

A. Violación directa del Código de Ética Profesional

El Código de Ética establece que es un catálogo de conductas exigidas y prohibidas para los ingenieros .

Firmar un acuerdo que obliga a:

- Ocultar delitos
- No denunciar actividades ilegales
- Participar o guardar silencio sobre cibercrimen

Esto implica una violación directa de las prohibiciones y deberes profesionales.

Además, el régimen disciplinario indica que:

“Será susceptible de sanción… todo acto… que implique… ejecución de actividades delictuosas… o violación de prohibiciones”

Es decir: Aceptar ese acuerdo podría constituir falta disciplinaria sancionable.

B. Incumplimiento de deberes éticos fundamentales

El código establece deberes como:

- Actuar con probidad, honestidad y responsabilidad
- Proteger a la sociedad
- Velar por el buen nombre de la profesión

Sin embargo, el acuerdo del Anexo 3 exige:

- Encubrir delitos informáticos
- No reportar actividades ilegales
- Aceptar prácticas como interceptación o espionaje

Esto va en contra de la responsabilidad social del ingeniero y la legalidad del ejercicio profesional.

C. Participación en actividades delictivas

El Código es claro en que: “Constituye falta disciplinaria el ejercicio de actividades delictuosas relacionadas con la profesión”

Firmar el acuerdo puede implicar complicidad o encubrimiento y participación indirecta en delitos informáticos; lo que no solo es una falta ética, sino también responsabilidad penal individual y riesgo de procesos judiciales.

D. Posibles sanciones disciplinarias

Según la Ley 842 de 2003 (Código de Ética del COPNIA), el profesional puede enfrentar:

- Amonestación escrita
- Suspensión de la matrícula profesional

- Cancelación de la matrícula (faltas gravísimas)

Y se consideran gravísimas, entre otras:

Incurrir en delitos relacionados con el ejercicio profesional

- En este caso, el acuerdo:
- Promueve delitos
- Obliga a encubrirlos

Lo cual podría llevar incluso a la cancelación definitiva de la matrícula profesional, afectando de manera crítica el desarrollo de las actividades propias del ejercicio de la profesión.

E. Afectación al ejercicio profesional y reputación

El COPNIA es la entidad encargada de:

- Vigilar el ejercicio profesional
- Investigar faltas éticas
- Sancionar a los ingenieros

Si el profesional firma y actúa bajo el acuerdo descrito en el Anexo 3:

- Puede ser denunciado ante el COPNIA
- Se afecta su reputación profesional
- Se limita su capacidad de ejercer legalmente

(*Código de Ética | Consejo Profesional Nacional de Ingeniería | Copnia*, 2026).

Análisis del caso problema "Ciberespionaje y Ética en SecureNova Labs" (Anexo 2 - Escenario 2), con punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar:

Desde una perspectiva profesional, SecureNova Labs incurre en una falta grave al no revisar los contratos elaborados por un abogado previamente cuestionado. Esto podría acarrearle:

- Riesgos legales: Por la inclusión en su acuerdo de confidencialidad de cláusulas abusivas, ilegales o que vulneran derechos fundamentales (como privacidad y protección de datos).
- Responsabilidad corporativa: La empresa es responsable por las actuaciones de su personal y los instrumentos jurídicos que utiliza, así quiera evadir su responsabilidad mediante la firma del acuerdo de confidencialidad.
- Riesgos éticos: Se afecta su reputación y se compromete la confianza de clientes (gobiernos y corporaciones) al no garantizar transparencia ni integridad en sus procesos.

Además, obligar a su personal bajo presión a realizar acceso a entornos con datos sensibles puede incentivar conductas inapropiadas si la organización no realiza controles estrictos, lo que podría desencadenar en actividades de ciberespionaje interno o abuso de privilegios.

Límite para las empresas de ciberseguridad relacionados con acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo garantizar que los accesos no sean explotados de manera indebida:

Debe establecerse para la información un “Principio de privilegio mínimo” el cual limita a la empresa de ciberseguridad a tener el acceso mínimo necesario con respecto a los datos sensibles de sus clientes. Para garantizar que con los datos entregados se realice un uso adecuado en cuanto a explotación, las organizaciones deben blindarse con mecanismos como contrato claros y auditados que contengan acuerdos de confidencialidad bien estructurados y aprobados legalmente, controlar los contratos en ejecución por medio de auditorías internas y externas; ambas con alcances claramente definidos. Técnicamente se deben establecer controles como registros de actividades (logs), monitoreo en tiempo real y segmentación de redes y datos que garanticen control efectivo.

Es muy importante que las organizaciones cuenten con políticas de seguridad alineadas con las regulaciones normativas y los marcos de referencia internacionales relacionados con seguridad

de la información, además del establecimiento en las cláusulas de los acuerdos de confidencialidad; de sanciones individuales por el uso indebido de la información sensible.

Mecanismos de supervisión y control que 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 el uso indebido de herramientas forenses o de hacking ético, las empresas de ciberseguridad deben implementar sistemas robustos de control que deben contener como mínimo los siguientes elementos:

Controles organizacionales

- Separación de funciones (Aprobador y validador no pueden ser la misma persona)
- Principio de doble control (4 ojos)
- Evaluaciones éticas periódicas al personal

Controles técnicos

- Monitoreo de uso de herramientas (Por medio de sistemas SIEM, EDR)
- Grabación de sesiones en entornos críticos
- Control de accesos basado en roles (RBAC)

Controles administrativos

- Código de ética profesional obligatorio
- Programas de concientización en ética
- Procedimientos disciplinarios claros

Auditoría continua

- Auditorías internas y externas
- Revisiones de logs y trazabilidad de acciones

Respuesta de los gobiernos y organizaciones cuando se evidencia que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje:

Si se confirma que una empresa de ciberseguridad ha cometido ciberespionaje, la respuesta debe ser contundente y estructurada, con la toma de acciones enfocadas no solo a proteger a la organización; sino sus activos de información y la posibilidad de responder penalmente de manera solidaria en los casos que no son de su alcance. Las acciones que deben tomarse son:

Acciones inmediatas

- Suspensión del contrato con la empresa implicada
- Investigación forense independiente
- Notificación a autoridades competentes

Acciones legales

- Aplicación de sanciones penales y civiles
- Demandas por daños y perjuicios
- Inclusión en listas de inhabilitación contractual

Medidas para restaurar la confianza

- Transparencia en la comunicación del incidente
- Auditorías externas certificadas
- Revisión completa de proveedores de ciberseguridad

Medidas preventivas

- Fortalecer marcos regulatorios
- Exigir certificaciones (ISO 27001, ISO 27701)
- Implementar controles de terceros

Medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente:

Es muy innecesario comprender que la restauración de la confianza no se logra por medio de acciones aisladas, son por medio de un proceso integral, verificable y durable en el tiempo; por esto es necesaria la combinación de medidas técnicas, legales, organizacionales y reputacionales que garanticen el manejo adecuado. Las medidas recomendadas son:

Acciones inmediatas (contención y transparencia): La transparencia temprana es clave: ocultar el incidente empeora la pérdida de confianza, lo primero es detener el daño y asumir la responsabilidad; para esto se propone:

- Suspensión o terminación inmediata del contrato con la empresa implicada
- Aislamiento de sistemas comprometidos
- Preservación de evidencia digital (cadena de custodia)
- Notificación a clientes, autoridades y partes afectadas

Responsabilidad legal y sanciones: En estos caso se hace necesario enviar un mensaje claro que permita advertir que el abuso de capacidades de ciberseguridad no queda impune, por esto es necesario establecer consecuencias judiciales que garanticen restablecer credibilidad, las adecuadas son:

- Procesos penales contra responsables directos
- Sanciones administrativas a la empresa
- Demandas por daños y perjuicios
- Inhabilitación para contratar con el Estado (si aplica)

Investigación forense independiente: Es necesario e importante garantizar objetividad y credibilidad técnica, no basta con una investigación interna. Se requiere:

- Auditoría forense por un tercero independiente
- Reconstrucción de la línea de tiempo del incidente
- Identificación de datos comprometidos

- Evaluación del alcance real del espionaje

Fortalecimiento de controles internos: Muchos de los casos de ciberespionaje logran materializarse por la falta de controles estrictos en la organización cliente, esta medida es muy importante para garantizar que no se repita y los controles recomendados son:

- Controles técnicos
  - Monitoreo continuo (SIEM, SOC)
  - Registro y auditoría de todas las actividades (logs)
  - Control de accesos bajo principio de mínimo privilegio
  - Segmentación de redes y datos sensibles
- Controles organizacionales
  - Separación de funciones (quien audita no ejecuta sin supervisión)
  - Modelo de “doble validación”
  - Evaluaciones de confianza y ética del personal
- Controles administrativos
  - Actualización del código de ética
  - Políticas estrictas de uso de herramientas ofensivas
  - Programas obligatorios de formación en ética y cumplimiento

Revisión de contratos y gobernanza: Otro de los aspectos que genera vacíos al proceso por ambigüedades documentales y que permiten la ocurrencia de casos de ciberespionaje, para evitarlo todo acceso debe estar justificado, documentado y auditable; el problema muchas veces nace en el marco contractual, por esto es importante:

- Redefinir los acuerdos de confidencialidad
- Establecer límites claros de acceso a la información
- Incluir cláusulas de auditoría y supervisión continua

- Definir sanciones específicas por uso indebido de datos

Certificaciones y cumplimiento normativo: No solo se evitan sanciones sino que se recupera la confianza al demostrar cumplimiento con estándares reconocidos:

- Implementación o fortalecimiento de ISO/IEC 27001 (seguridad de la información)
- ISO/IEC 27701 (privacidad)
- Marcos como NIST o CIS

(Leonardo, 2018) (National Institute of Standards and Technology |*NIST*, 2018) (Compleye.io, 2025).

Además:

- Auditorías externas periódicas
- Publicación de informes de cumplimiento

Gestión de terceros (Third-Party Risk Management): Trabajar con terceros implica que la organización deba conocerlos y reforzar el control sobre sus proveedores externos porque no debe confiarse solo en su reputación sino que debe contarse con controles verificables, existen procesos establecidos:

- Evaluaciones de seguridad antes de contratar
- Auditorías legal y reputacional
- Monitoreo continuo del proveedor
- Limitación estricta de accesos

Cultura organizacional y ética: En muchas de las organizaciones la prevención a largo plazo no es posible porque depende de la cultura, este aspecto debe fortalecerse mediante las siguientes acciones:

- Promover una cultura de ética profesional
- Canales de denuncia protegidos

- Incentivar el comportamiento responsable
- Liderazgo comprometido con la transparencia

Estrategia de comunicación y reputación: Al igual que es importante asumir las responsabilidades, para restaurar la confianza pública es necesario establecer acciones que la garanticen; estas son:

- Comunicación clara, honesta y sin ambigüedades
- Explicación de medidas correctivas implementadas
- Reportes periódicos de avances
- Participación en auditorías públicas o regulatorias

(CALDER, 2017) (*ISO 27001 Frente al Marco de Ciberseguridad Del NIST: ¿Cuál Es La Diferencia?*, 2025)

Ejercicio de pentesting para el desarrollo de capacidades de equipos red team y blue team

Componente práctico

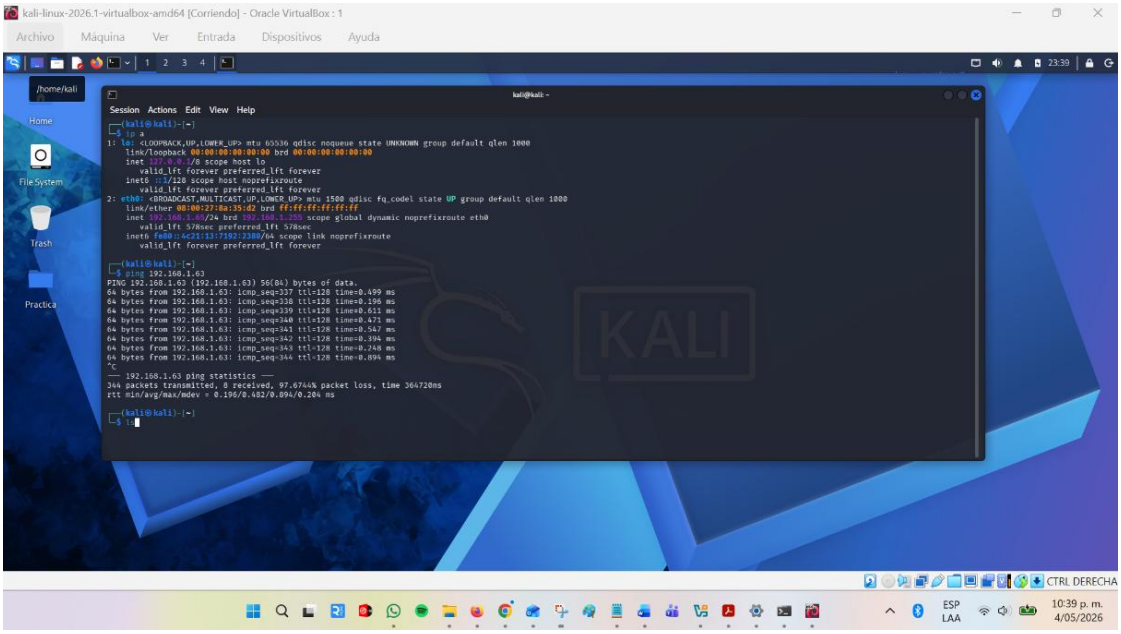
Con el problema que se encuentra en el Anexo 4 – Escenario 3 referente a equipo red team y por medio del banco de trabajo configurado previamente deberá darse respuesta a las siguientes preguntas orientadoras:

- Describir de manera específica las herramientas software que se utilizan para llevar a cabo el Anexo 4 – Escenario 3 enfocado a red team. Deberá adjuntarse evidencia de los comandos utilizados y resultados arrojados en cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.
  - Reconocimiento: Se inicia con una consola de comandos para identificar la IP existente en cada máquina virtual (verificación que ya se había realizado anteriormente en el ejercicio de la preparación del banco de trabajo), en esta misma se realiza “ping” de una

maquina a otra (Kali Linux a Host A) y viceversa para garantizar que se encuentren en una misma red y que respondan los ping enviados en ambos sentidos. En la Figura 10 puede observarse inicialmente la configuración de la tarjeta de red “eth0” existente para la máquina Kali Linux, la cual tiene la dirección IP 192.168.1.65/24 y habiendo identificado la dirección IP 192.168.1.63/24 para el Host A en el alistamiento del banco de trabajo, se procede a enviar un ping para verificar que pueda alcanzarse esta segunda máquina desde la máquina virtual Kali Linux.

Figura 10

Identificación de IP de Kali Linux y ping respondiendo desde Host A



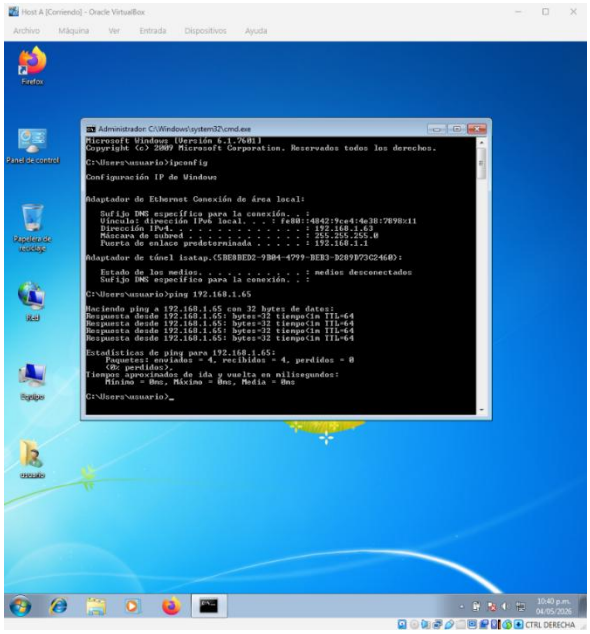
Nota. Verificación de conectividad entre las máquinas virtuales enviando ping mediante consola de comandos desde la máquina Kali Linux con respuesta de la máquina Windows 7, la figura es de autoría del propio autor.

También es necesario e importante realizar desde el Host A el mismo procedimiento para comprobar que la conectividad existente entre las dos máquinas virtuales es funcional y que no existe en ninguna de las dos; restricción alguna que impida la realización del ejercicio de

pentesting propuesto. En la Figura 11 se observa inicialmente la identificación de la dirección IP del Host A 192.168.1.63/24 y la respuesta al ping enviado a la máquina Kali Linux.

Figura 11

Identificación de IP de Host A y ping respondiendo desde Kali Linux



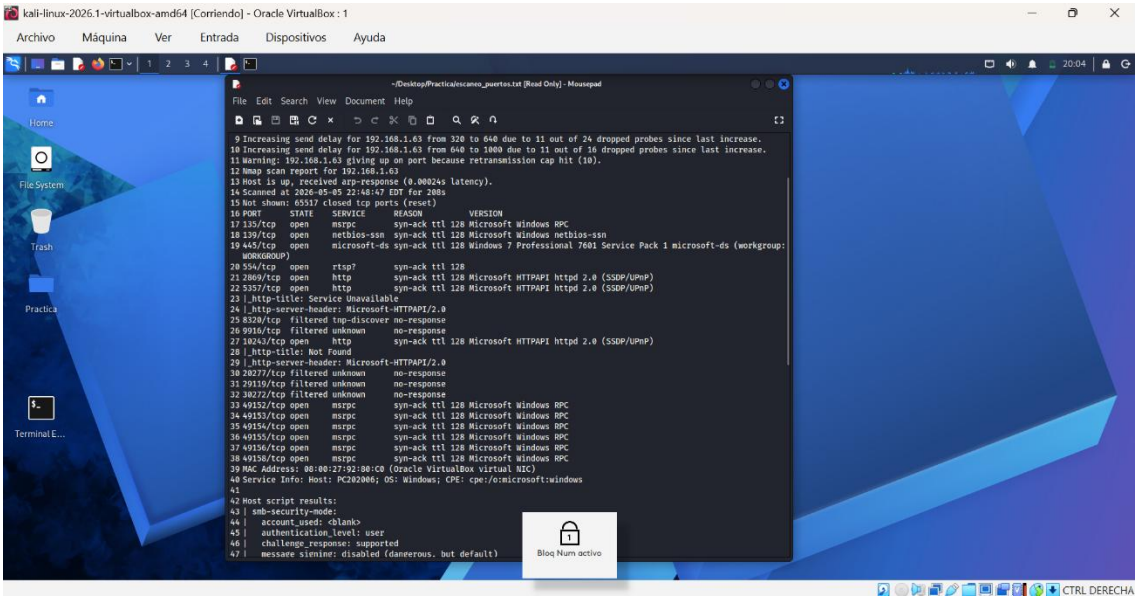
Nota. Verificación de conectividad entre las máquinas virtuales enviando ping mediante consola de comandos desde la máquina Windows 7 con respuesta de la máquina Kali Linux, la figura es de autoría del propio autor.

Con la seguridad que las máquinas pueden verse, pueden iniciarse las acciones iniciales de reconocimiento como lo es el escaneo de puertos que se realiza por medio de Nmap desde Kali Linux direccionado a la IP 192.168.1.63 correspondiente al Host A para identificar puertos abiertos y servicios que puedan estar generando acceso a software malicioso. De lo observado en la Figura 12 resulta útil para el ejercicio de pentesting toda la información que permita establecer los puertos abiertos como el caso del 445/tcp por medio del cual en los procesos siguientes se pueden direccionar las acciones para lograr la identificación de las vulnerabilidades existentes la manera de explotarlas para obtener el acceso con privilegios solicitado que finalmente permitirá

la vulneración de los demás equipos interconectados aunque no se encuentren en la misma red en la que se encuentran el Host A y la máquina Kali Linux, pues al ser vulnerado el Host A; este sirve de puente (pivoting) para realizar la vulneración de los demás equipos.

Figura 12

Resultado de Nmap ejecutado desde Kali Linux a la IP de Host A para escaneo de puertos



Nota. Resultado de Nmap mediante consola de comandos desde la máquina Kali Linux con relación a la IP del Host A, la figura es de autoría del propio autor.

- Escaneo de vulnerabilidades: En este punto y sabiendo que el Host A puede ser atacado, puede realizarse un escaneo de vulnerabilidades también por medio de Nmap enviado desde Kali Linux hacia la IP del Host A; precisamente para lograr la identificación de las vulnerabilidades existentes y por medio de las mismas, encontrar la manera de realizar la explotación para acceder con privilegios y poder realizar cambios en el Host A. En este caso el resultado del escaneo se puede observar en la Figura 13, con lo siguientes resultados:

  Host script results:

|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

| smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

| Disclosure date: 2017-03-14

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

|_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

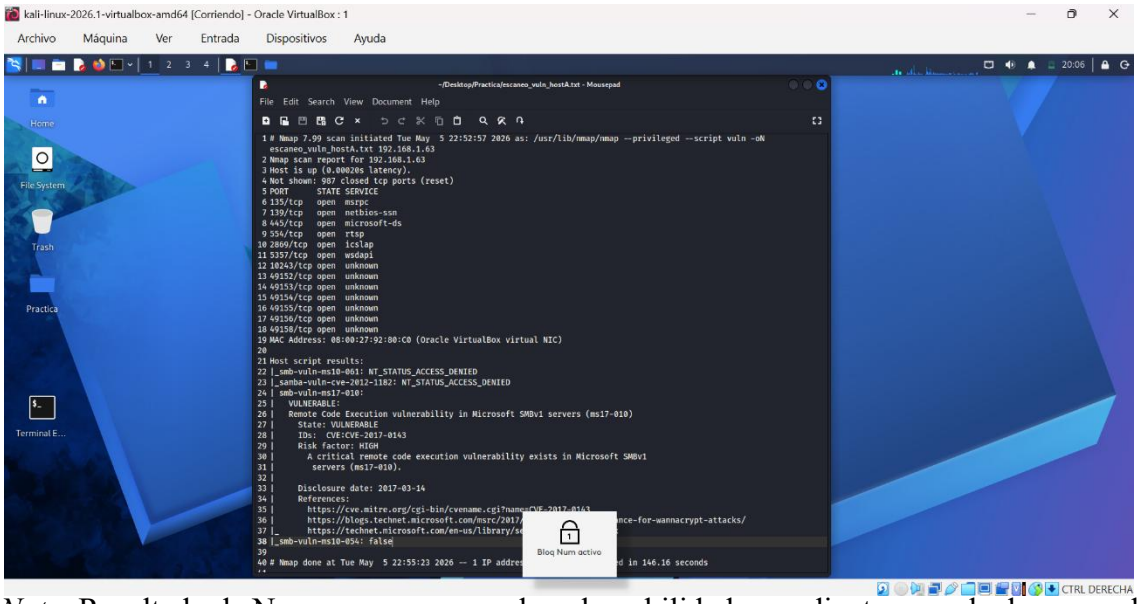
|_smb-vuln-ms10-054: false

El texto resaltado en amarillo extraído del "Host script results" permite la identificación de una vulnerabilidad explotable debido a que consiste en que el Host A tiene habilitado SMBv1 y es vulnerable a la falla explotada históricamente por malware como WannaCry (ataca cifrando archivos valiosos para que no pueda accederse a ellos, o bien bloqueando el acceso al ordenador para inutilizarlo). Esta es precisamente la vulnerabilidad que puede explotarse para llevar a buen término la realización del proceso de ataque ejecutado por el red team que terminará concediendo acceso al Host A y a los recursos necesarios para continuar con la explotación de la

vulnerabilidad para llagar al objetivo final que es la explotación del Host B y generar cambios en su configuración (Rapid7.Com, 2026).

Figura 13

Resultado de Nmap ejecutado desde Kali Linux a la IP de Host A para escaneo de vulnerabilidades



Nota. Resultado de Nmap para escaneo de vulnerabilidades mediante consola de comandos desde la máquina Kali Linux con relación a la IP del Host A, la figura es de autoría del propio autor.

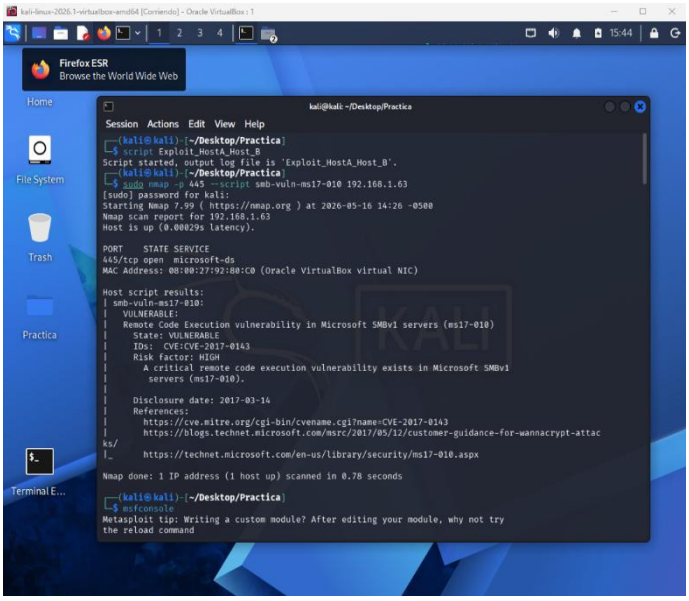
- Explotación: La vulnerabilidad encontrada permite:
  - Ejecución remota de código (RCE)
  - Movimiento lateral
  - Escalada de privilegios
  - Instalación de malware/ransomware

En este caso puede explotarse la vulnerabilidad identificada por medio del código “sudo Nmap -p 445 –script smb-vuln-ms17-010 192.168.1.63” como se observa en la Figura 14, en la misma puede observarse una explotación efectiva en 0,78 segundos de la IP vulnerable con lo cual es posible ejecutar Metasploit por medio del comando “msfconsole” para luego indicar la

vulnerabilidad a explotar con el comando “use exploit/Windows/smb/ms17_010_eternalblue”, además de configurar el Host de lectura (set RHOSTS 192.168.1.63) y el Host de escucha (set LHOST 192.168.1.65); finalmente se ejecuta el comando “exploit” para materializar la explotación.

Figura 14

Ejecución de Nmap ejecutado desde Kali Linux a la IP de Host A



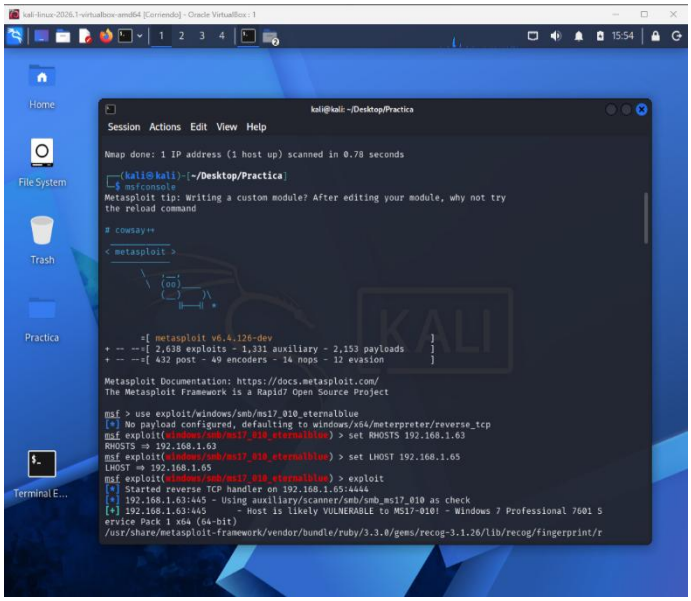
Nota. Ejecución de Nmap para inicio de explotación de vulnerabilidades mediante consola de comandos desde la máquina Kali Linux con relación a la IP del Host A, la figura es de autoría del propio autor.

En la Figura 15 y de acuerdo a lo solicitado en el ejercicio, debería demostrarse el movimiento lateral entre Host A y Host B; por medio de Metasploit (msfconsole) se realizan diferentes procedimientos como la apertura de una sesión Meterpreter sobre el puerto 445/tcp del Host A y por medio de este, ejecutar el movimiento lateral (pivoting) para alcanzar el Host B que se encuentra conectado al Host A por medio de una red diferente a la existente con la máquina atacante y demostrar por medio del proceso de red team la importancia de identificar, explotar y mitigar la vulnerabilidades existentes para garantizar la seguridad no solo de la red que el

atacante logra alcanzar sino que al acceder a uno de los equipos de la organización, dependiendo sus configuraciones, y los demás equipos que interactúan con este; puede causar potenciales daños a la infraestructura crítica en general de la organización (Figuras 16, 17, 18 y 19).

Figura 15

Ejecución de msfconsole y parametrización para explotación de la vulnerabilidad encontrada



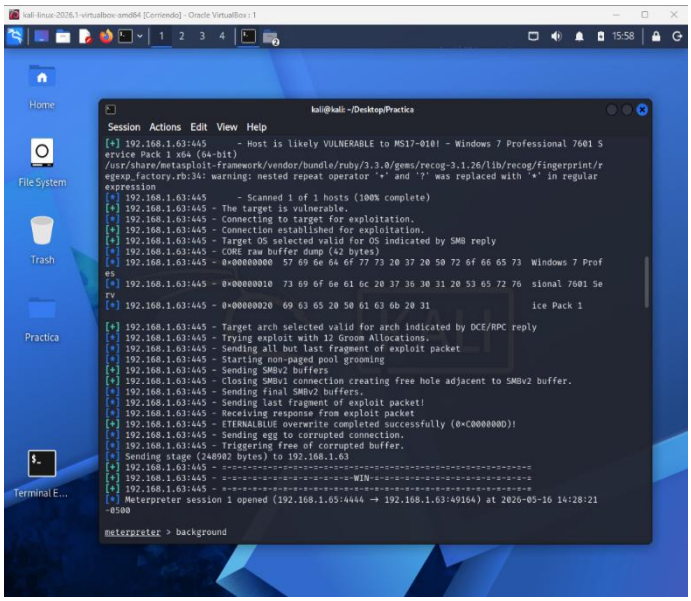
Nota. Resultados de ejecución de msfconsole mediante consola de comandos para explotación de vulnerabilidades desde la máquina Kali Linux con relación a la IP del Host A, la figura es de autoría del propio autor.

En la figura anterior se observa la ejecución de Metasploit dentro de la consola de comandos de la máquina Kali Linux direccionada hacia el Host A que de acuerdo con las fases anteriores, se tiene identificada como la máquina con vulnerabilidades explotables. Se observan las respectivas configuraciones para lograr el proceso de explotación y puede verificarse que fue exitoso al final de la consola de comandos donde se observa que en el puerto 445 de la máquina asociada a la dirección IP 192.168.1.63 (Host A) se puede realizar una explotación efectiva de la vulnerabilidad conocida como MS17-010, la cual es una falla atribuible a la infección del Host A

con el archivo HFS; la cual es conocida como EternalBlue, ampliamente utilizada para ejecución remota de código y propagación de malware como WannaCry.

Figura 16

Apertura de sesión Meterpreter en msfconsole



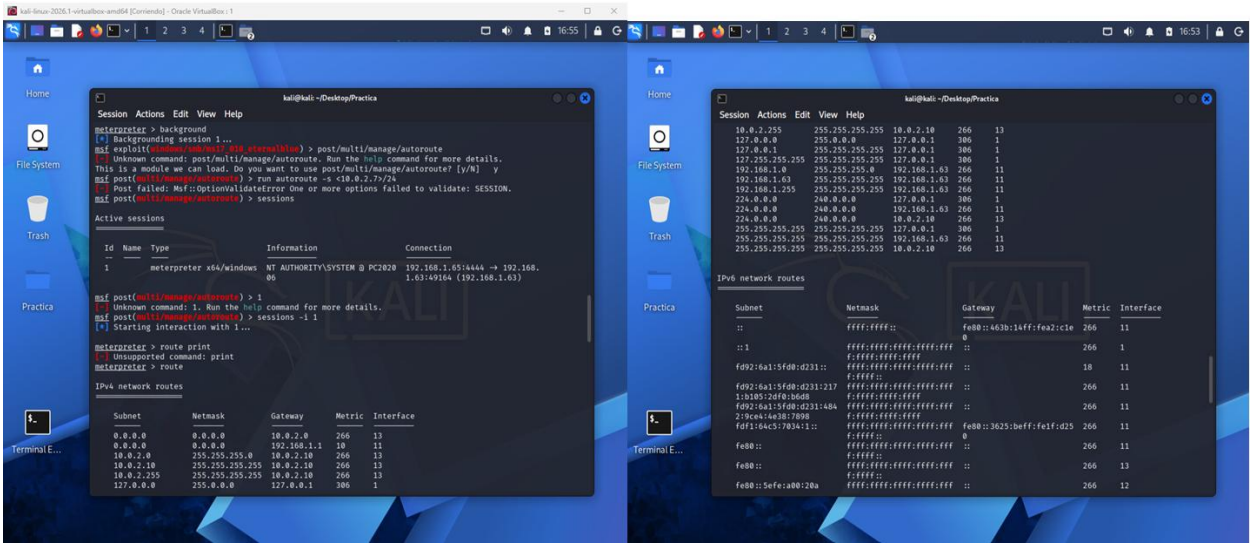
Nota. Apertura de sesión en msfconsole que permite explotación de la vulnerabilidades mediante consola de comandos desde la máquina Kali Linux con relación a la IP del Host A, la figura es de autoría del propio autor.

Una sesión Meterpreter es una conexión avanzada y dinámica que se establece normalmente tras la explotación exitosa de una vulnerabilidad mediante el Metasploit. Esta sesión proporciona al especialista o pentester una interfaz interactiva para controlar de forma remota el sistema comprometido (Host A), permitiendo ejecutar comandos, gestionar archivos, recopilar información del sistema, escalar privilegios y realizar tareas de post-explotación. Desde máquina Kali Linux, el usuario puede interactuar con Meterpreter a través de comandos especializados para enumerar procesos, capturar credenciales, inspeccionar configuraciones de red y evaluar el alcance del acceso obtenido, todo dentro de un entorno controlado orientado a la validación de vulnerabilidades y al análisis de seguridad que para el caso puntual; consiste en alcanzar el Host B, obtener privilegios de administrador y realizar cambios notorios para

demostrar la vulneración del Host a través de un ataque direccionado a un equipo diferente que por medio de sus vulnerabilidades pone en riesgo toda la red.

Figura 17

Ejecución de comandos en msfconsole para llegar a la red de Host B

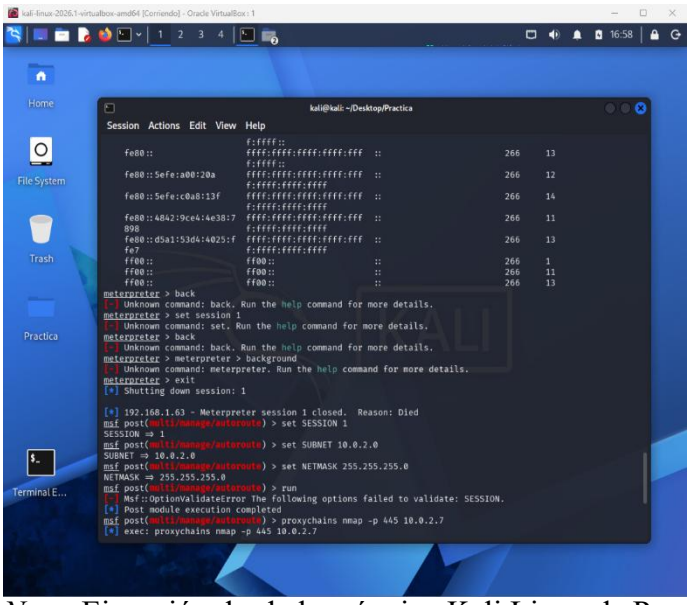


Nota. Alcance del Host B desde la máquina Kali Linux por medio del Host A (pivoting) realizado mediante consola de comandos, la figura es de autoría del propio autor.

La sesión de Meterpreter obtenida desde Kali Linux puede permitir el acceso indirecto a equipos ubicados en segmentos de red distintos mediante técnicas de pivoteo o movimiento lateral. Esto ocurre cuando la máquina atacante compromete primero un sistema intermedio vulnerable a EternalBlue (asociado a la vulnerabilidad MS17-010 en Windows), logrando establecer control sobre dicho equipo. Una vez comprometida esta máquina intermedia, actúa como puente entre redes, permitiendo al analista especializado realizar reconocimiento interno, identificar nuevos activos y validar el alcance de acceso hacia sistemas que inicialmente no eran visibles desde la red de origen. Este proceso permite evaluar riesgos relacionados con segmentación deficiente, propagación lateral y exposición de servicios internos dentro de una infraestructura corporativa; de tal manera que estos riesgos no permitan que un atacante cause afectaciones a los activos de información de la organización.

Figura 18

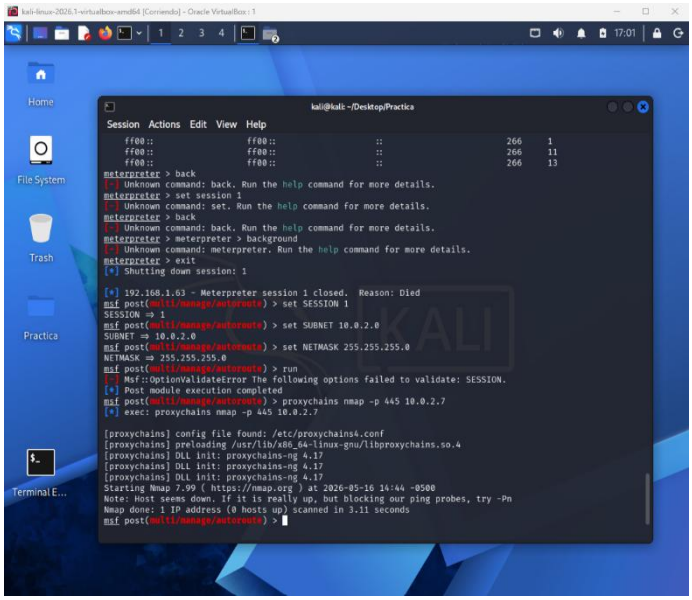
Ejecución de ProxyChains en msfconsole



Nota. Ejecución desde la máquina Kali Linux de ProxyChains en consola de comandos por medio del Host A (pivoting) para llegar al Host B, la figura es de autoría del propio autor.

ProxyChains es una herramienta utilizada en Kali Linux para redirigir el tráfico de red de aplicaciones a través de uno o varios servidores, permitiendo enrutar conexiones hacia redes que no son accesibles directamente desde la máquina atacante. En una sesión de Meterpreter gestionada desde Metasploit, ProxyChains se emplea comúnmente después de comprometer una máquina intermedia, configurando dicha máquina como punto de pivote para alcanzar otros equipos en segmentos de red internos. De esta manera, herramientas de reconocimiento, escaneo o validación ejecutadas desde la consola de Kali Linux pueden enviar su tráfico a través del túnel establecido por Meterpreter, simulando que las conexiones provienen desde el sistema comprometido. Esto resulta especialmente útil en ejercicios de pentesting para evaluar escenarios de movimiento lateral, segmentación de red y exposición de servicios internos en entornos controlados.

Figura 19
Resultado de ProxyChains en msfconsole



Nota. Resultados de ProxyChains desde la máquina Kali Linux por medio del Host A (pivoting) para llegar al Host B, la figura es de autoría del propio autor.

En la imagen se configura un módulo de enrutamiento para realizar pivoting hacia una red interna, definiendo la subred 10.0.2.0 con máscara 255.255.255.0, posteriormente se utiliza ProxyChains para redirigir el tráfico de red y ejecutar un escaneo con Nmap hacia la dirección 10.0.2.7 sobre el puerto 445 (SMB). El resultado del escaneo indica que el host objetivo (Host B) está activo, aunque con restricciones en la detección por bloqueo de sondas ICMP, y confirma que el puerto 445 se encuentra accesible, lo que evidencia conectividad hacia la red remota y la posibilidad de continuar con actividades de reconocimiento o validación de servicios expuestos.

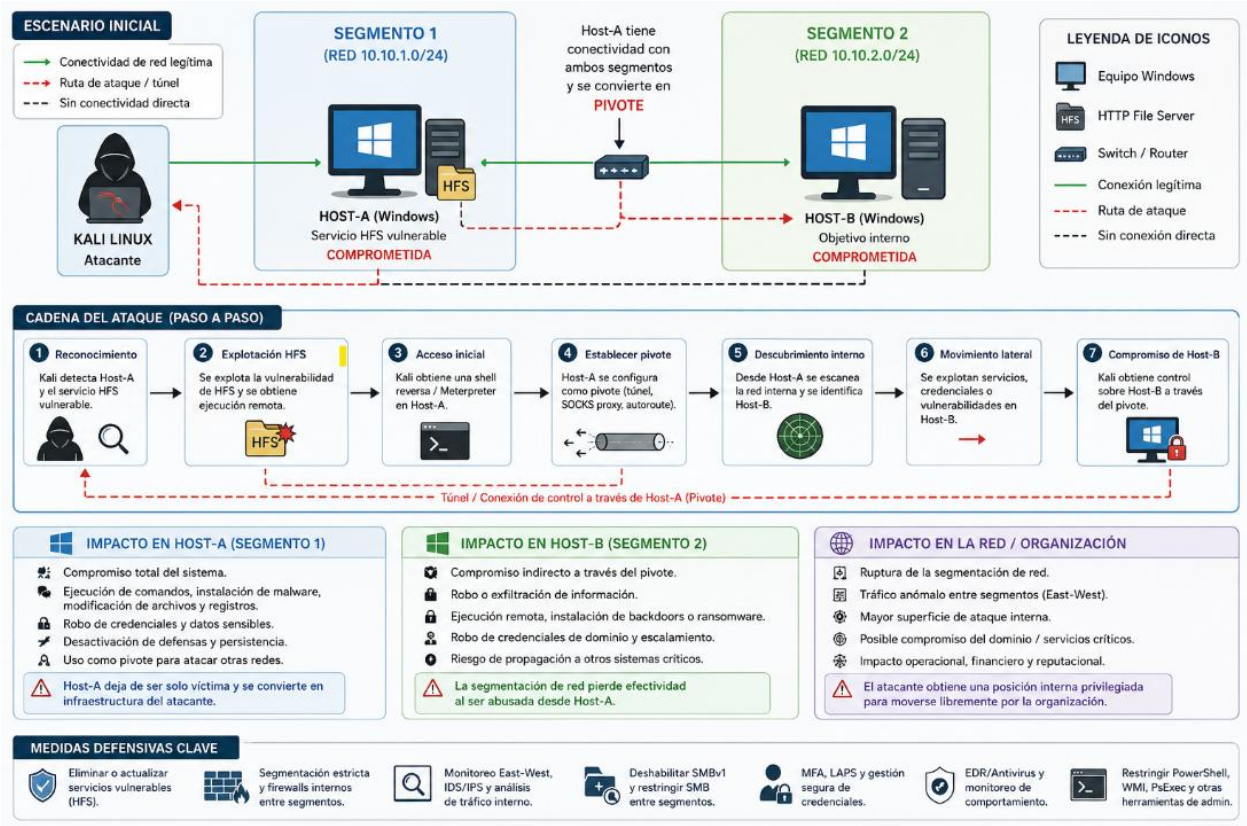
- Post-Explotación: Logrando el movimiento lateral entre los Host A y B, es posible la creación de usuarios con privilegios de manera remota y con estos vulnerar al Host B como se solicita en el ejercicio y realizar cualquier explotación luego de alcanzar dicho equipo como se explica gráficamente a continuación (Figura 20). Lo más importante de la fase de post-explotación es verificar que otras afectaciones podría sufrir el sistema en

general con la vulneración realizada, verificar si por ejemplo el segmento donde se encuentra el Host B permite vulnerar otros equipos de la red o si la segmentación existente permite contener el movimiento lateral.

Este tipo de ejercicios es muy útil porque permite establecer las debilidades de los sistemas informáticos y enfocar los esfuerzos en ciberseguridad para contrarrestar y/o mitigar los ataques que puedan poner en riesgo las infraestructuras de redes y comunicación de una organización (Bharat Kotwani et al., 2023).

Figura 20

Explicación gráfica de afectación ocurrida en Host A y Host B



Nota. Detalle de los procesos ejecutados dentro del ejercicio de pentesting para lograr la vulneración del Host B sin que este se encuentre en el mismo segmento de red de la máquina atacante (Kali Linux), la figura es de autoría del propio autor creada con la ayuda de IA (*ChatGPT*, 2026).

- Datos e información del Anexo 4 – Escenario 3 que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la Máquina - 1 Windows.

De acuerdo con el anexo se sugiere que podrían estar realizándose movimientos laterales, creación de usuarios con permisos administrativos y todo esto por la existencia de una aplicación vulnerable. Con el desarrollo del ejercicio y basado en el contenido del anexo propuesto, pudo utilizarse la información de la existencia de un servidor de archivos o base de datos que fue el que generó la vulnerabilidad explotable. Con la vulnerabilidad identificada e incluso solo con el hecho de saber que existe un servidor "hfs" se puede consultar en la web lo que significa tener esta condición en un equipo de la red y las posibilidades de explotación de vulnerabilidades que podrían intentarse.

- Herramienta utilizada para identificar los fallos de seguridad de la Máquina - 1 Windows y puerto que abre la aplicación específica en el anexo.

Nmap, para el caso de estudio muestra varios puertos abiertos por medio de los cuales podrían ocurrir explotaciones, pero para el caso puntual se puede evidenciar que en el puerto 445/tcp está corriendo el servidor y la aplicación que generan los accesos maliciosos por medio de los cuales se puede ejecutar la explotación.

- Explicación de la afectación por el ataque a las máquinas (Windows) encontradas en la red: Haga uso de gráficos para explicar el ataque.

Segmentos involucrados

  - Segmento 1:
    - Kali Linux (atacante)
    - Host-A Windows vulnerable con HFS

- Segmento 2:
  - Host-B Windows objetivo final

Inicialmente, Kali NO tiene acceso directo a Host-B porque:

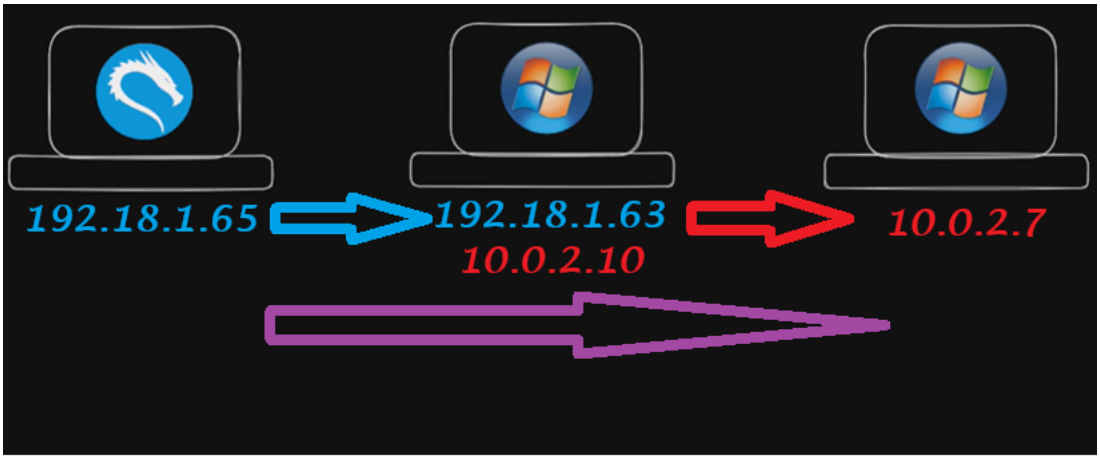
- Están en redes diferentes
- Probablemente existe segmentación
- Host-B no enruta tráfico directamente hacia Kali.

Sin embargo, Host-A sí tiene conectividad con ambos segmentos, convirtiéndose en un "puente" involuntario para el atacante.

Al lograrse la vulneración del Host B es posible la explotación que se describe en la Figura 20.

Figura 21

Explicación gráfica del proceso de explotación realizado



Nota. Afectación de las máquinas Windows (Host A y Host B), por explotación realizada desde máquina Kali Linux, la figura es de autoría del propio autor.

Respuesta y Contención ante Incidentes de Ciberseguridad

Con en el Anexo 5 – Escenario 4 referente a equipo blue team y por medio banco de trabajo configurado en el apartado anterior se generan los siguientes planteamientos:

Acciones prioritarias al encontrarse un ataque en tiempo real, respuesta especificada con argumentos técnicos:

La primera acción recomendada para el equipo blue team es la contención del incidente sin destruir evidencia, porque un ataque en ejecución puede continuar propagándose, robando información o realizando movimiento lateral hacia otros segmentos de red. Como parte de la contención se deben realizar los siguientes procesos prioritarios iniciales:

A. Determinar el alcance del incidente: Es muy importante identificar: El equipo comprometido, proceso(s) en ejecución, usuario que ejecuta archivos maliciosos, conexiones de red activas, otros equipos que se están comunicando con el equipo afectado. Para el caso de estudio se identificó el Host A como el equipo que permitió la vulneración, generando esto la afectación del Host b, ambos deben aislarse y asegurarse para obtener la mayor información posible del incidente.

B. Aislar el equipo comprometido: El equipo donde se detectó la ejecución de HFS debe mantenerse encendido para facilitar el análisis forense de memoria RAM, debe desconectarse de la red corporativa y bloquearse desde el firewall y/o switch. Es importante no apagar el equipo comprometido porque con esto puede destruirse evidencia importante como sesiones activas, conexiones TCP, procesos maliciosos, Shell reversas, credenciales temporales y payloads cargados en la memoria.

C. Revisión de conexiones activas y procesos: Es importante la verificación de procesos activos, en ejecución y de conexiones establecidas con el equipo afectado por medio de la utilización de comandos como: tasklist, netstat -ano, Get-Process y la utilización de herramientas recomendadas para estos procesos de identificación como TCPView, Sysmon, Process Explores y Wireshark; el objetivo de este procedimiento es la identificación de puertos abiertos, procesos

de persistencia, túneles o reverse shell, ip atacante y en el caso puntual; procesos asociados al ejecutable HFS.

D. Identificación de las implicaciones de la explotación conocida de HFS: Este tipo de falla de seguridad posee vulnerabilidades históricas como: Ejecución de código remoto (RCE), descarga remota de malware, reverse shell vía HTTP y ejecución mediante scripts o Powershell. Es muy importante que el blue team revise archivos descargados recientemente, tareas programadas, usuarios creados, logs de Windows Event Viewer, servicios nuevos y cambios en privilegios.

E. Verificar movimiento lateral (pivoting): Debido a que se identificó la afectación de un equipo perteneciente a un segmento de red diferente al utilizado públicamente por el equipo comprometido, es importante que se realicen análisis adicionales sobre uso de SMB, PsExec, Pass-the-Hash, RPD, WinRM, WMI, robo de credenciales y realizar especial investigación de net user, net localgroup administrators y quser.

F. Recolectar la evidencia: El blue team debe recolectar y garantizar la preservación de logs, capturas de tráfico, memoria RAM, indicadores de compromiso (IOC), imagen forense de disco, hashes; proceso en los que suelen utilizarse herramientas especializadas en análisis forense como Autopsy, Volatility, FTK Imager, Magnet RAM Capture. (Panda Security, 2019).

Medidas de hardenización propuestas para que el ataque no se repita, teniendo en cuenta el ataque ejecutado desde el ejercicio de red team:

Después de detectado el incidente es muy importante la implementación de medidas de hardening tanto en Windows como en la red, las más recomendadas son:

A. Eliminar o actualizar HFS vulnerable: En caso de necesitarse el HFS deben desinstalarse versiones vulnerables, restringir su exposición a internet y utilizar únicamente versiones

actualizadas. Para el caso puntual, debe eliminarse ya que se instaló en el Host A como un archivo malicioso.

B. Segmentación de red: Debido a que se detectó la afectación de un equipo en un segmento diferente al direccionamiento de la IP del equipo comprometido es importante restringir el tráfico SMB/RDP entre segmentos, implementación de VLANs, aplicación de listas de control de acceso (ACL), aplicación de modelos de cero confianza (zero trust).

C. Deshabilitación de servicios innecesarios: Una medida preventiva es la eliminación o deshabilitación de servicios no requeridos y que pueden favorecer la ocurrencia de ataques como telnet, SMB, servicios HTTP innecesarios y powershell remoto no autorizado en todos los equipos afectados (Host A y Host B para este caso).

D. Aplicación de políticas de mínimo privilegio: Deben establecerse políticas de restricción de privilegios como: los privilegios de administradores locales no deben darse a todos los usuarios, restricción de binarios desconocidos y aplicación de control de cuentas de usuario estricto (UAC).

E. Implementar listas blancas de aplicaciones: Es un procedimiento que garantiza que solo puedan ejecutarse programas preaprobados y de confianza en la red y sus dispositivos, para impedir la ejecución de herramientas no autorizadas y malware. Para esto se utilizan herramientas como Windows Defender Application Control y AppLocker.

F. Hardening del sistema operativo: Es importante la aplicación permanente de:

- Actualizaciones de seguridad.
- Parches críticos.
- Deshabilitación de macros.
- Protección antiexploit.
- Windows Defender avanzado.

G. Monitoreo continuo: Uso de herramientas de monitoreo continuo como:

- SIEM.
- Sysmon.
- IDS/IPS.
- EDR/XDR.

H. Reglas de firewall restrictivas: Políticas de Firewall para bloqueo de puertos no utilizados, comunicación entre segmentos innecesaria y tráfico saliente sospechoso.

En la siguiente tabla 1 se explican las medidas de hardenización:

Tabla 1
Medidas de hardenización para evitar ataques

Medida de Hardening	Descripción	Objetivo de Seguridad	Aplicación Práctica
A. Eliminación o actualización de HFS vulnerable	Consiste en remover versiones vulnerables de HFS o actualizar a versiones seguras con parches aplicados.	Evitar explotación de vulnerabilidades de acceso remoto y ejecución de código.	Desinstalar versiones obsoletas, restringir acceso externo y limitar exposición del servicio solo a redes autorizadas.
B. Segmentación de red	Separación lógica o física de redes para evitar propagación lateral entre segmentos.	Minimizar movimiento lateral del atacante dentro de la infraestructura.	Implementar VLANs, ACLs, políticas Zero Trust y restringir tráfico SMB/RDP entre segmentos.

C. Deshabilitación de servicios innecesarios	Eliminación o desactivación de servicios que no aportan al negocio y aumentan superficie de ataque.	Reducir vectores de intrusión y exposición innecesaria.	Deshabilitar servicios como Telnet, SMBv1, HTTP no requerido y PowerShell remoto no autorizado.
D. Políticas de mínimo privilegio	Asignación de permisos mínimos necesarios para usuarios, aplicaciones y administradores.	Limitar el impacto de cuentas comprometidas.	Restringir privilegios administrativos, reforzar UAC y controlar ejecución de binarios no confiables.
E. Listas blancas de aplicaciones	Permite ejecutar únicamente software previamente autorizado y validado.	Bloquear malware, herramientas no autorizadas y ejecución de payloads maliciosos.	Implementar AppLocker o Windows Defender Application Control.
F. Hardening del sistema operativo	Aplicación de controles de seguridad sobre el sistema operativo y sus configuraciones.	Fortalecer la resistencia frente a ataques conocidos y explotación de vulnerabilidades.	Aplicar actualizaciones, parches críticos, protección anti-exploit, deshabilitar macros y fortalecer Microsoft Defender.

G. Monitoreo continuo	Supervisión constante de eventos, tráfico y comportamiento de endpoints.	Detectar tempranamente actividad maliciosa o comportamiento anómalo.	Implementar SIEM, Sysmon, IDS/IPS y plataformas EDR/XDR para visibilidad centralizada.
H. Reglas de firewall restrictivas	Definición de políticas estrictas para controlar tráfico entrante, saliente e interno.	Bloquear comunicaciones no autorizadas y limitar propagación del ataque.	Cerrar puertos innecesarios, bloquear tráfico sospechoso y restringir comunicación entre segmentos no requerida.

Nota. Principales medidas de hardenización después de materializado un ataque. Fuente: *Marco de Ciberseguridad 4.2*, (2022).

Diferencias entre un equipo blue team y un equipo de respuesta a incidentes informáticos:

El equipo de respuesta a incidentes normalmente puede hacer parte del blue team, pero tiene un enfoque más especializado en manejo de crisis, análisis forense, contención avanzada y recuperación operativa. Puede confundirse la función entre uno y otro pero son diferentes desde el punto de vista operativo como se observa en el siguiente comparativo:

Tabla 2
Comparativo blue team - Equipo de respuesta a incidentes informáticos

Aspecto	Blue team	Equipo de Respuesta a Incidentes
Objetivo principal	Defensa continua	Gestionar incidentes específicos

Aspecto	Blue team	Equipo de Respuesta a Incidentes
Trabajo	Permanente	Reactivo
Función	Monitoreo, prevención y detección	Contención, erradicación y recuperación
Herramientas	SIEM, IDS, EDR, firewalls	Forense, análisis malware, recuperación
Enfoque	Seguridad operativa	Manejo técnico del incidente
Tiempo de actuación	Continuo	Durante y después del incidente

Nota. Revisión comparativa en varios aspectos entre un blue team y un Equipos de respuesta a incidentes informáticos.

Utilización de CIS "Center For Internet Security", dentro de un equipo blue team:

Center for Internet Security se utiliza principalmente para implementar estándares de seguridad, configuraciones seguras, controles de hardening y buenas prácticas de ciberseguridad. En la utilización de CIS se establecen controles priorizados para prevenir ataques, mejorar monitoreo y reducir superficie de ataque, controles como inventario de activos, gestión de vulnerabilidades, control de privilegios y monitoreo de logs. Por medio de marcos de referencias internacionales se definen guías técnicas para hardening de Windows, Linux, Firewalls, Bases de datos, Cloud, Dispositivos de red.

Por medio de CIS el blue team puede realizar evaluaciones de cumplimiento para validar configuraciones inseguras, servicios vulnerables, permisos excesivos, configuraciones débiles y

la aplicación de CIS permite reducir la superficie de ataque para deshabilitar servicios innecesarios, endurecer políticas, limitar privilegios y aumentar trazabilidad. (Saed et al., 2025).

Funciones y características principales de lo que es un SIEM:

Un SIEM es una plataforma de seguridad que centraliza, correlaciona y analiza eventos provenientes de múltiples dispositivos y sistemas. Sus funciones principales son:

A. Recolección de logs: Recibe eventos desde servidores, firewalls, switches, antivirus, Active Directory, endpoints y aplicaciones.

B. Correlación de eventos: Relaciona múltiples eventos para detectar ataques complejos como múltiples intentos fallidos, autenticación exitosa, ejecución de PowerShell, conexión externa sospechosa.

C. Detección de amenazas: Detecta malware, ransomware, fuerza bruta, movimiento lateral y exfiltración.

D. Generación de alertas: Notifica al blue team en tiempo real. Notifica en tiempo real al blue team para que puedan tomarse acciones inmediatas

E. Monitoreo centralizado: Permite realizar supervisión en tiempo real de toda la infraestructura desde un único panel.

F. Retención de evidencias: Almacena logs e información importante para auditorías, cumplimiento y análisis forense.

G. Características principales

Tabla 3
Características de SIEM

Característica	Descripción
Centralización	Consolida eventos de múltiples fuentes

Característica	Descripción
Correlación	Relaciona eventos complejos
Escalabilidad	Soporta grandes volúmenes de logs
Automatización	Respuestas automáticas
Visibilidad	Monitoreo en tiempo real
Forense	Conservación de evidencias
Integración	Compatible con IDS, EDR, firewalls

Nota. Características principales y su descripción para Security Information and Event Management (SIEM).

Los SIEM más conocidos y usualmente más demandados en la actualidad son:

- Splunk Enterprise Security
- IBM QRadar
- Microsoft Sentinel
- Wazuh
- Elastic Security

(National Institute of Standards and Technology, 2018).

La utilización de un SIEM en SecureNova Labs habría permitido detectar el tráfico inusual entre los equipos afectados, el movimiento lateral, la ejecución remota de comandos y demás actividades sospechosas permitiendo actuar a tiempo para prevenir la vulneración d ellos sistemas informático de la organización

3 herramientas de contención de ataques informáticos “hardware o software”, teniendo en cuenta que las herramientas de contención son diferentes a las herramientas de detección:

Las herramientas de contención buscan detener, limitar o aislar un ataque activo. Son diferentes de las herramientas de detección. Algunas de ellas son:

A. Firewall

Función: Controlar y bloquear tráfico de red.

Capacidades de contención: Bloqueo de IP atacante, cierre de puertos, restricción entre segmentos, bloqueo de conexiones salientes maliciosas.

Ejemplos de Firewall: Fortigate, pfSense, Windows Defender Firewall.

B. EDR (Endpoint Detection and Response)

Función: Contener amenazas directamente en endpoints.

Capacidades de contención: Aislamiento automático del host, finalización de procesos maliciosos, cuarentena de archivos, bloqueo de ejecución.

Ejemplos de EDR: Microsoft Defender for Endpoint, CrowdStrike Falcon, SentinelOne.

C. NAC (Network Access Control)

Función: Controlar qué dispositivos pueden acceder a la red.

Capacidades de contención: Aislar dispositivos comprometidos, mover hosts a VLAN de cuarentena, revocar acceso automáticamente.

Ejemplos de NAC: Cisco Identity Services Engine y Aruba ClearPass.

D. IPS (Intrusion Prevention System)

Función: Bloquear tráfico malicioso automáticamente.

Capacidades de contención: Bloqueo de exploits, detección de firmas, prevención de movimiento lateral.

Ejemplos de IPS: Snort, Suricata.

Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/j1D327CfXS0

Conclusiones

El desarrollo del laboratorio permitió identificar vulnerabilidades críticas presentes en una infraestructura tecnológica simulada, evidenciando cómo la exposición de servicios inseguros como HFS puede convertirse en un vector inicial de ataque con impacto significativo sobre la seguridad organizacional.

Mediante actividades de reconocimiento y escaneo con herramientas como Nmap fue posible identificar servicios expuestos, puertos abiertos y posibles superficies de ataque, facilitando la evaluación técnica de riesgos asociados a la infraestructura analizada.

La explotación controlada de vulnerabilidades mediante Metasploit permitió establecer una sesión Meterpreter sobre Host A, demostrando la viabilidad de ejecución remota de comandos y el compromiso inicial del sistema vulnerable.

El uso de técnicas de pivoting y herramientas como ProxyChains evidenció cómo un atacante puede desplazarse lateralmente entre segmentos de red, comprometiendo activos adicionales como Host B cuando no existen controles adecuados de segmentación y monitoreo.

Desde la perspectiva blue team, se evidenció que la respuesta efectiva ante incidentes requiere una combinación de capacidades técnicas y organizacionales orientadas al aislamiento, contención, preservación de evidencia, análisis forense y fortalecimiento continuo de controles de seguridad.

La segmentación de red, el hardening, la gestión de parches, el monitoreo centralizado mediante SIEM y la implementación de soluciones EDR e IDS/IPS constituyen controles fundamentales para reducir la superficie de ataque y mejorar la capacidad de detección temprana.

No existe una metodología única y universal para la ejecución de pruebas de pentesting, ya que su alcance depende del entorno, los objetivos, las reglas de enfrentamiento y las

herramientas utilizadas. Sin embargo, existen marcos de referencia ampliamente reconocidos que orientan su ejecución técnica y metodológica.

El análisis del caso SecureNova Labs permitió comprender que el ejercicio de la ciberseguridad no depende únicamente de capacidades técnicas, sino también del cumplimiento de principios éticos, legales y profesionales que garanticen el uso responsable del conocimiento.

Recomendaciones

Medidas inmediatas

Actualizar de forma prioritaria los sistemas operativos, aplicaciones y servicios expuestos para corregir vulnerabilidades críticas identificadas durante el ejercicio, especialmente aquellas asociadas a HFS y protocolos inseguros.

Deshabilitar servicios obsoletos o inseguros como SMBv1, eliminando componentes vulnerables que puedan facilitar ejecución remota de código o movimiento lateral.

Implementar procedimientos de aislamiento inmediato para equipos comprometidos, reduciendo el riesgo de propagación hacia otros segmentos de red.

Medidas de mediano plazo

Fortalecer la segmentación de red mediante VLANs, ACLs y controles de acceso que limiten el desplazamiento lateral entre activos críticos.

Implementar soluciones SIEM para centralizar logs, correlacionar eventos y detectar comportamientos anómalos asociados a escaneo, explotación o movimientos laterales.

Desplegar herramientas EDR e IDS/IPS que permitan identificar actividad maliciosa en endpoints, conexiones sospechosas y posibles intentos de persistencia.

Medidas permanentes

Realizar pruebas periódicas de pentesting y ejercicios controlados de red team y blue team para evaluar continuamente la postura de seguridad.

Implementar procesos permanentes de revisión de configuraciones, hardening, validación de parches y eliminación de software vulnerable.

Fortalecer la capacitación del personal técnico y administrativo en buenas prácticas de ciberseguridad, respuesta a incidentes y protección de activos de información.

Establecer métricas de seguimiento mediante auditorías, revisión de logs, simulaciones de incidentes y nuevos escaneos de vulnerabilidades que permitan validar la efectividad de los controles implementados. (Chindruş & Căruntu, 2023).

Referencias Bibliográficas

Chindrus, C., & Caruntu, C.-F. (2023). *Securing the Network A Red and Blue Cybersecurity Competition Case Study. Information* , 14(11), 587. https://doi-org.bibliotecavirtual.unad.edu.co/10.2478/bipie-2023-0008

Compleye.io. (2025) *ISO 27001 frente al Marco de Ciberseguridad del NIST: ¿Cuál es la diferencia?* https://compleye.io/es/articulos/iso-27001-vs-nist-cybersecurity-framework-cual-es-la-diferencia

Congreso de la República de Colombia. (2009, 5 de enero). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Ministerio de Relaciones Exteriores de Colombia*. https://www.cancilleria.gov.co/normograma/compilacion/docs/ley_1273_2009

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Departamento Administrativo de la Función Pública.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Copnia. (2015). *Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares* . Copnia (pp. 3–26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia* [Monografía]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/41392

INCIBE. (2021). *Pentesting* | INCIBE | Incibe.es. https://www.incibe.es/aprendeciberseguridad/pentesting

INCIBE. (2019). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas* . INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditandoseguridad-tus-sistemas

Iso27, A. (2017). *ISO27001/ISO27002: Una guía de bolsillo*. https://doi.org/10.2307/j.ctt1pwt92r

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). *Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. International Journal of Scientific Research in Engineering and Management*, 7(12), 1–11. https://doi.org/10.55041/IJSREM27675

Leonardo. (2018, November 13). *Guía de seguridad de la información basada en la norma ISO 27001 y el estándar NIST-IR 7621 revisión 1 del National Institute Of Standards And Technology para pymes, con diseño de políticas para la empresa profesionales Asociados Ltda.* Udistrital.Edu.Co. https://repository.udistrital.edu.co/items/7f67bd64-e938-4e01-a05a-36d4bd08e78a

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/

Marco de Ciberseguridad 4.2. (2022). *Agencia de Gobierno Electrónico Y Sociedad de La Información Y Del Conocimiento*. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad-42

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (2022). *Políticas de Privacidad y Condiciones de Uso*. https://www.mintic.gov.co/portal/inicio/Secciones

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Framework for Improving Critical Infrastructure Cybersecurity*, 1.1(1). https://doi.org/10.6028/nist.cswp.04162018

OpenAI. (2026). *ChatGPT* (modelo GPT-5.5). https://chatgpt.com

Oracle. (2026). Oracle VM *Virtualbox.* https://www.virtualbox.org/

PandaSecurity. (2018). *Pentesting: Una herramienta muy valiosa para tu empresa* . Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentestingherramienta-empresa/

Presidencia de la República de Colombia. (2013, 27 de junio). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Departamento Administrativo de la Función Pública.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Presidencia de la República de Colombia. (2014, 13 de mayo). *Decreto 886 de 2014: Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Departamento Administrativo de la Función Pública.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Presidencia de la República de Colombia. (2015, 26 de mayo). *Decreto 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Departamento Administrativo de la Función Pública.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608

Rapid7. (2026). *Metasploitable 2 | Metasploit Documentation*. https:// https://docs.rapid7.com/metasploit/metasploitable-2

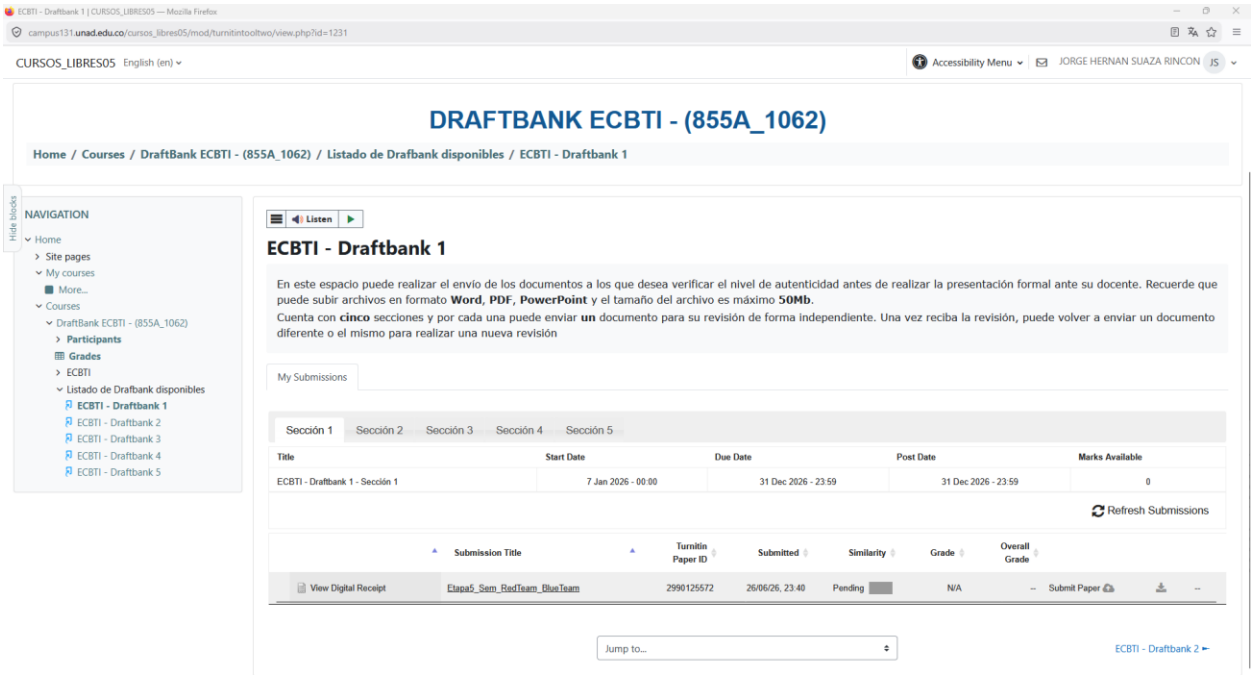
Saed, R., Guadalupe, C., Minaya, W., & Ediciones Gesicap. (2025, February 27). *Fundamentos de Seguridad Informática y Ciberseguridad*. https://www.researchgate.net/publication/389395515_Fundamentos_de_Seguridad_Informatica_y_Ciberseguridad

Trigos, E. (2026). *[Grabación de webconferencia No. 2 – Taller Práctico (Fase 3 Red Team)]*. Sharepoint.Com. https://unadvirtualedu-my.sharepoint.com/personal/eduvin_trigos_unad_edu_co/_layouts/15/stream.aspx?id=%2Fpersonal%2Feduvin_trigos_unad_edu_co%2FDocuments%2FRecordings%2FWebconferencia+No.+2+%E2%80%93+Taller+Pr%C3%A1ctico+%28Fase+3+Red+Team%29-20260428_201337-Grabaci%C3%B3n+de+la+reuni%C3%B3n.mp4&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0&ga=1&referrer=StreamWebApp.Web&referrerScenario=AddressBarCopied.view.899679c0-5eb5-447f-b664-62c7acc5ec50

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Captura de verificación en plataforma Turnitin para revisión del porcentaje de similitud del informe con material existente en las bases de datos y/o la web en general.