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

Javier Andres Tamara Hadechine

Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team

Director Curso

Luis Fernando Zambrano Hernandez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias básicas, tecnología e ingeniería – ECBTI

Especialización en Seguridad Informática

Bogotá

22 Mayo 2025

Resumen

El presente informe técnico tiene como propósito documentar el análisis, la ejecución y la reflexión crítica sobre una serie de escenarios simulados en ciberseguridad, desarrollados en el contexto organizacional de *CyberFort Technologies*. A lo largo de cuatro etapas se aborda el diseño de un banco de pruebas con software libre, la identificación de amenazas y vulnerabilidades mediante técnicas de pentesting, el análisis ético y legal de contratos laborales en entornos tecnológicos, y la contención de un ataque informático real en tiempo de ejecución. El informe integra herramientas como Metasploit, Nmap, Enum4linux, Wireshark y Volatility, así como referencias normativas relevantes como la Ley 1273 de 2009 y la Ley 1581 de 2012. La estructura metodológica empleada permite evidenciar no solo las capacidades técnicas del profesional, sino también su integridad y criterio ético frente a situaciones límite, alineándose con las exigencias contemporáneas del ejercicio responsable en ciberseguridad.

Palabras clave

Análisis forense, Blue Team, Ciberseguridad, Pentesting, Red Team.

Abstract

The purpose of this technical report is to document the analysis, execution, and critical reflection on a series of simulated cybersecurity scenarios developed within the organizational context of CyberFort Technologies. The four stages address the design of a testbed using open source software, the identification of threats and vulnerabilities using pentesting techniques, the ethical and legal analysis of employment contracts in technological environments, and the containment of a real cyberattack at runtime. The report integrates tools such as Metasploit, Nmap, Enum4linux, Wireshark, and Volatility, as well as relevant regulatory references such as Law 1273 of 2009 and Law 1581 of 2012. The methodological framework employed demonstrates not only the professional's technical capabilities but also their integrity and ethical judgment in the face of extreme situations, aligning with contemporary demands for responsible cybersecurity practice.

Keywords:

Blue Team, Cybersecurity, Digital forensics, Pentesting, Red Team.

Tabla de contenido

Lista de Figuras

Lista de tablas

Glosario

CIS Benchmarks: Guías técnicas desarrolladas por el Center for Internet Security para asegurar configuraciones óptimas en sistemas y dispositivos.

EternalBlue (MS17-010): Vulnerabilidad crítica en SMBv1 explotable en versiones antiguas de Windows, asociada con ataques tipo ransomware y ejecución remota de código.

Ley 1273 de 2009: Reforma al Código Penal colombiano que tipifica los delitos informáticos y protege la información y los datos.

Ley 1581 de 2012: Regula el tratamiento de datos personales en Colombia, garantizando los derechos al hábeas data y a la privacidad.

Pentesting: Proceso estructurado para evaluar la seguridad de un sistema mediante la simulación de ataques informáticos controlados.

Red Team / Blue Team: Metodologías complementarias en ciberseguridad. El Red Team simula ataques; el Blue Team se encarga de la defensa y respuesta.

SIEM (Security Information and Event Management): Plataforma que centraliza y correlaciona eventos de seguridad, facilitando la detección y respuesta ante incidentes.

Introducción

El avance de las amenazas cibernéticas exige no solo habilidades técnicas avanzadas, sino también una sólida comprensión ética y legal por parte de los profesionales en ciberseguridad. Este informe documenta el desarrollo progresivo de actividades simuladas en el entorno de CyberFort Technologies, donde se evaluó la capacidad del ingeniero para desplegar entornos de prueba, identificar vulnerabilidades reales, aplicar marcos legales y normativos vigentes, y responder a incidentes bajo condiciones críticas. Cada etapa pone a prueba la integridad técnica y moral del profesional, situándolo en contextos reales donde el conocimiento, la ética y la legalidad convergen.

Planteamiento del Problema

En la era digital contemporánea, las organizaciones enfrentan un entorno altamente vulnerable a amenazas cibernéticas que comprometen la confidencialidad, integridad y disponibilidad de la información. La transformación digital, el uso de servicios en la nube, dispositivos IoT y el teletrabajo han ampliado la superficie de ataque, haciendo necesaria la implementación de estrategias ofensivas y defensivas (CIS, 2021).

CyberFort Technologies, compañía que asesora entidades gubernamentales en seguridad informática, ha evidenciado fallos estructurales al no contar con equipos formalizados de Red Team y Blue Team. Entre los hallazgos más críticos se encuentra el uso de sistemas operativos obsoletos como Windows 7 con SMBv1 activo, que son vulnerables a exploits como MS17-010, los cuales permiten ejecución remota de código sin autenticación (NIST, 2012).

Esta situación no solo pone en riesgo la infraestructura tecnológica, sino que también puede derivar en el incumplimiento de normativas como la Ley 1273 de 2009, que penaliza el acceso no autorizado, la interceptación de datos y el uso de software malicioso (Congreso de Colombia, 2009), así como la Ley 1581 de 2012, que regula el tratamiento de datos personales y exige medidas de seguridad adecuadas (Congreso de Colombia, 2012). La falta de mecanismos de respuesta a incidentes, el uso indebido de cláusulas contractuales y la carencia de monitoreo forense evidencian una debilidad institucional que compromete tanto la legalidad como la ética profesional.

Justificación

La elaboración de este informe técnico se justifica por la necesidad de fortalecer un enfoque integral en la práctica de la ciberseguridad, que incluya no solo la competencia técnica, sino también la observancia de los marcos legales vigentes y la ética profesional. En efecto, el ejercicio responsable de roles dentro de equipos Red Team y Blue Team requiere una actuación coherente con principios jurídicos y códigos deontológicos, tal como lo exige el Código de Ética del COPNIA y la Ley 842 de 2003.

La promoción del uso de herramientas open source como Wazuh, Wireshark o Metasploit permite además optimizar recursos en contextos con presupuesto limitado, manteniendo altos estándares de protección (Wazuh, 2024). Adicionalmente, el marco NIST SP 800-61r2 proporciona una guía metodológica para gestionar incidentes de forma estructurada, asegurando contención, recolección de evidencia y restauración de servicios (NIST, 2012).

El caso de CyberFort Technologies permite analizar cómo la omisión de estas prácticas puede derivar en incumplimientos legales y en escenarios éticamente cuestionables. Por tanto, este informe no solo desarrolla capacidades técnicas, sino que contribuye a la formación de profesionales capaces de actuar con integridad, dentro de los límites de la ley y en beneficio de la protección institucional y ciudadana (OEA, 2025).

Objetivo general:

Diagnosticar y fortalecer las capacidades técnicas, legales y éticas de los equipos Red Team y Blue Team en el entorno organizacional de CyberFort Technologies, mediante la simulación de escenarios reales de ciberseguridad, con el fin de detectar vulnerabilidades, contener amenazas y garantizar el cumplimiento normativo.

Objetivos específicos:

1. **Etapa 1 – Banco de trabajo y fundamentos legales:**

   Diseñar un entorno virtual de pruebas con herramientas open source, garantizando la conectividad, funcionalidad y sustentación legal necesaria para el desarrollo de simulaciones de ciberseguridad.

2. **Etapa 2 – Evaluación legal y ética:**

   Analizar la legalidad y ética de los contratos propuestos por CyberFort Technologies, identificando cláusulas abusivas y riesgos jurídicos conforme a la legislación colombiana y al Código de Ética profesional.

3. **Etapas 3 y 4 – Simulación Red Team y Blue Team:**

   Desarrollar ejercicios prácticos de ciberseguridad que incluyan pruebas de penetración y respuesta a incidentes, aplicando metodologías ofensivas (Red Team) y defensivas (Blue Team) para evidenciar vulnerabilidades, contener ataques y preservar evidencia forense.

4. **Entrega del informe técnico final:**

   Elaborar y entregar un informe técnico integral a CyberFort Technologies, consolidando hallazgos, análisis normativos y recomendaciones estratégicas que fortalezcan su postura de seguridad informática.

DESARROLLO DEL INFORME TECNICO

Etapa 1 Conceptos de equipos de seguridad

Margen legal en Colombia

En colombia la regulación de la ciberseguridad, los delitos informáticos y el tratamiento de datos personales se articula a través de un marco normativo robusto que ha evolucionado como respuesta al impacto de las tecnologías de la información en la sociedad. Este marco se fundamenta principalmente en la Ley 1273 de 2009, la Ley 1581 de 2012, el Decreto 1377 de 2013 y la Ley 1266 de 2008, así como en los principios rectores del Código de Ética Profesional (Ley 842 de 2003) para ingenieros en ejercicio.

La Ley 1273 de 2009, considerada el pilar de la legislación penal informática en Colombia, modificó el Código Penal e incorporó el Título VII BIS: "De los delitos informáticos y contra la protección de la información y de los datos". Esta norma tipifica conductas como el acceso no autorizado a sistemas informáticos (art. 269A), la interceptación ilícita de datos (art. 269C), el uso de software malicioso (art. 269E) y la violación de datos personales (art. 269F), entre otros (Fun09) .Su enfoque se centra en proteger la confidencialidad, integridad y disponibilidad de la información, reconociéndola como un bien jurídico autónomo.

Complementariamente, la Ley 1581 de 2012 establece el régimen general de protección de datos personales en Colombia. Esta norma desarrolla el derecho fundamental al hábeas data consagrado en la Constitución Política, garantizando a los ciudadanos el control sobre el uso de su información personal. Establece principios rectores como legalidad, finalidad, libertad,

veracidad, seguridad y confidencialidad, además de otorgar a la Superintendencia de Industria y Comercio (SIC) funciones de inspección, vigilancia y control (Congreso de Colombia, 2012).

El Decreto 1377 de 2013, reglamentario de la Ley 1581, refuerza estos principios al establecer procedimientos para la autorización, recolección, almacenamiento y tratamiento de datos personales. Asimismo, promueve el desarrollo de políticas de privacidad y mecanismos efectivos de gestión del riesgo informático, lo cual es fundamental en entornos corporativos donde se implementan simulaciones ofensivas (Red Team) o defensivas (Blue Team).

En contextos donde interviene información financiera o crediticia, se debe considerar también la Ley 1266 de 2008, que regula el habeas data financiero y establece derechos específicos sobre el reporte, actualización y eliminación de información en centrales de riesgo.

Desde una perspectiva profesional, el Código de Ética del COPNIA (Ley 842 de 2003) impone obligaciones claras a los ingenieros en ciberseguridad, entre ellas: actuar con independencia y probidad, denunciar irregularidades, abstenerse de encubrir delitos, y priorizar el interés público sobre el particular (artículos 31, 32 y 34).

Tabla 1. Artículos relevantes de la ley 1273 de 2009

Artículo	Contenido / Descripción	Relevancia para la Ciberseguridad
Artículo 1	Introduce el Título VII bis en el Código Penal: “De los delitos	Crea un nuevo bien jurídico que reconoce la importancia de la

	Artículo	Contenido / Descripción	Relevancia para la Ciberseguridad
		informáticos y contra la protección de la información y de los datos”	información digital como bien a proteger.
269A	Artículo	Acceso no autorizado a sistemas informáticos	Penaliza el acceso no autorizado a un sistema informático protegido. Base del delito de intrusión (hacking).
269B	Artículo	Obstrucción a sistemas informáticos o redes de telecomunicaciones	Sanciona conductas como el sabotaje a sistemas TI o ataques de denegación de servicio (DoS).
269C	Artículo	Intercepción de datos informáticos	Tipifica la interceptación de datos sin autorización. Aplica a sniffing, wiretapping, etc.
269D	Artículo	Daño informático	Penaliza la destrucción, daño o alteración de información digital. Se relaciona con malware o destrucción de backups.

	Artículo	Contenido / Descripción	Relevancia para la Ciberseguridad
269E	Artículo	Uso de software malicioso	Sanciona a quien produzca, adquiera o distribuya software malicioso (malware, virus, etc.).
269F	Artículo	Violación de datos personales	Protege la integridad y confidencialidad de los datos personales, alineado con el derecho fundamental al habeas data.
269G	Artículo	Suplantación de sitios web para capturar datos personales (phishing)	Penaliza la creación de páginas falsas para capturar datos. Es crucial en fraudes por ingeniería social.
9	Artículo	Modificación del artículo 250 de la Constitución y reformas al procedimiento penal	Asegura que la Fiscalía investigue de oficio los delitos informáticos. Refuerza la acción penal.

Fuente: Propia.

Artículos relevantes de la Ley 1581 de 2012

Artículo 1 – Objeto:

Regula el derecho fundamental al *hábeas data* (protección de datos personales).

Artículo 2 – Ámbito de aplicación:

Aplica a cualquier tratamiento de datos personales en Colombia o bajo jurisdicción colombiana.

Artículo 4 – Principios del tratamiento:

Establece principios como: legalidad, finalidad, libertad, veracidad, seguridad y confidencialidad.

Artículo 8 – Derechos del titular:

Permite al titular conocer, actualizar, rectificar y suprimir sus datos, además de revocar autorizaciones.

Artículo 17 – Deberes del responsable:

Define obligaciones para quien decide sobre el tratamiento, como garantizar la seguridad y actualizar los datos.

Artículo 18 – Deberes del encargado:

Regula las obligaciones del encargado del tratamiento bajo instrucciones del responsable.

Artículo 19 – Autoridad de control:

La *Superintendencia de Industria y Comercio* vigila el cumplimiento de esta ley.

Artículo 23 – Sanciones:

Establece sanciones administrativas por el mal uso o tratamiento indebido de datos.

Artículo 25 – Registro Nacional de Bases de Datos (RNBD):

Crea un registro público de bases de datos con acceso abierto a la ciudadanía.

Artículo 26 – Transferencia internacional de datos:

Restringe la transferencia a países sin niveles adecuados de protección, salvo excepciones.

Etapas del pentesting.

Las pruebas de penetración, también conocidas como penetration testing, constituyen un proceso estructurado para evaluar la seguridad de sistemas informáticos mediante la simulación controlada de ataques reales, conforme a metodologías reconocidas como OWASP, PTES y NIST SP 800-115 (Orebaugh, 2008). Este procedimiento se divide en varias etapas:

Reconocimiento o Recolección de Información: En esta fase, este recopilar la mayor cantidad de información posible sobre el objetivo antes de iniciar cualquier ataque. Se pueden usar técnicas de *OSINT* (Open Source Intelligence) para identificar direcciones IP, subdominios, servicios en ejecución, sistemas operativos y posibles vulnerabilidades.

Una de las herramientas que se usa para esta etapa es *Maltego*, una plataforma de recolección de datos que permite visualizar relaciones entre direcciones IP, dominios, correos electrónicos y más.

Análisis y Escaneo de Vulnerabilidades: En esta etapa, se identifican los puertos abiertos, servicios en ejecución y posibles vulnerabilidades explotables en el sistema objetivo. Se utilizan herramientas de escaneo para detectar fallos de configuración o software desactualizado.

Una de las herramientas que más se usa para estos casos es *Nmap*, ya que es un escáner de red que permite descubrir puertos abiertos y servicios activos en los sistemas objetivo.

Explotación o Ataque: Se intenta aprovechar las vulnerabilidades descubiertas para obtener acceso no autorizado a la red, sistema o aplicación. Se pueden utilizar exploits conocidos o desarrollar ataques específicos para vulnerabilidades detectadas en la fase anterior.

La herramienta más sonada para estos casos es *Metasploit Framework*, un conjunto de herramientas que permite ejecutar ataques contra sistemas vulnerables de manera automatizada o personalizada.

Mantenimiento del Acceso (Post-Explotación): Si se logra acceder a un sistema, el siguiente paso es establecer mecanismos de persistencia para mantener el control sobre el mismo, evitando que la víctima detecte la intrusión. En esta etapa, los atacantes pueden instalar *backdoors* o elevar privilegios dentro del sistema.

Empire Framework, es una herramienta que se usa como una plataforma de post-explotación que permite ejecutar comandos y mantener acceso remoto sin ser detectado fácilmente.

Análisis y Generación de Reporte: esta última fase consiste en documentar todas las actividades realizadas durante la prueba de penetración. Se incluyen detalles de las vulnerabilidades encontradas, los métodos utilizados para explotarlas y recomendaciones para corregir los problemas de seguridad.

Herramientas de ciberseguridad

Metasploit

Es un *framework* que te permite probar vulnerabilidades en sistemas, desarrollar exploits y hasta mantener acceso en una máquina comprometida (Rapid7, 2023).

¿Para qué sirve?

Pruebas de penetración: Simular ataques reales para ver si un sistema es vulnerable.

Desarrollo de exploits: Si encuentras un fallo, puedes crear un exploit para demostrarlo.

Post-explotación: Una vez dentro, se puede mover por la red o instalar puertas traseras.

Nmap

Herramienta que ayuda a descubrir qué dispositivos están conectados, qué puertos tienen abiertos y hasta qué sistema operativo usan. Es útil para hacer reconocimiento antes de un ataque o para auditar tu propia red (Nmap Project, 2023).

¿Para qué sirve?

Escaneo de puertos: Saber qué servicios están corriendo (ej. SSH, HTTP, FTP).

Detección de OS: Adivinar si un equipo usa Windows, Linux, etc.

Scripts avanzados: Se puede automatizar pruebas de vulnerabilidad con *NSE* (Nmap Scripting Engine).

OpenVAS

Es un escáner de vulnerabilidades de código abierto desarrollado inicialmente como parte de la iniciativa Greenbone Vulnerability Management (GVM). Esta herramienta permite identificar debilidades en sistemas operativos, aplicaciones, servicios y configuraciones de red, utilizando una base de datos constantemente actualizada con más de 80,000 pruebas conocidas como Network Vulnerability Tests (NVTs) (openvas.org, 2025)

¿Para qué sirve?

Escaneo automático: Revisa redes, servidores y aplicaciones en busca de fallos.

Informes detallados: Da un reporte con las vulnerabilidades y su nivel de riesgo.

Alternativa gratuita: Funciona como Nessus, pero sin la necesidad de una licencia paga.

ExploitDB

Es una plataforma de libre acceso que recopila exploits y pruebas de concepto (*Proof of Concept* - PoC) asociadas a vulnerabilidades de seguridad documentadas públicamente. Administrada por la comunidad de Offensive Security, ExploitDB actúa como una biblioteca técnica que centraliza miles de registros clasificados según vulnerabilidades, sistemas afectados y referencias como los identificadores CVE (Offensive Security, 2023).

¿Para qué sirve?

Buscar exploits: Tiene miles de códigos listos para usar.

Investigación: Sirve para entender cómo funcionan los ataques.

Pentesting: Si se descubre un CVE, se puede ver si ya hay un exploit público.

CVE

Es una nomenclatura estandarizada, mantenida por The MITRE Corporation con apoyo de la Cybersecurity and Infrastructure Security Agency (CISA), que permite identificar y catalogar vulnerabilidades de seguridad en sistemas informáticos mediante un código único y universalmente reconocido (cve25). Su objetivo es facilitar la interoperabilidad entre bases de datos, herramientas de escaneo, plataformas SIEM y marcos normativos, estableciendo un lenguaje común entre investigadores, desarrolladores, administradores de sistemas y equipos de respuesta a incidentes.

¿Para qué sirve?

Identificar vulnerabilidades: Saber si un sistema tiene un fallo conocido.

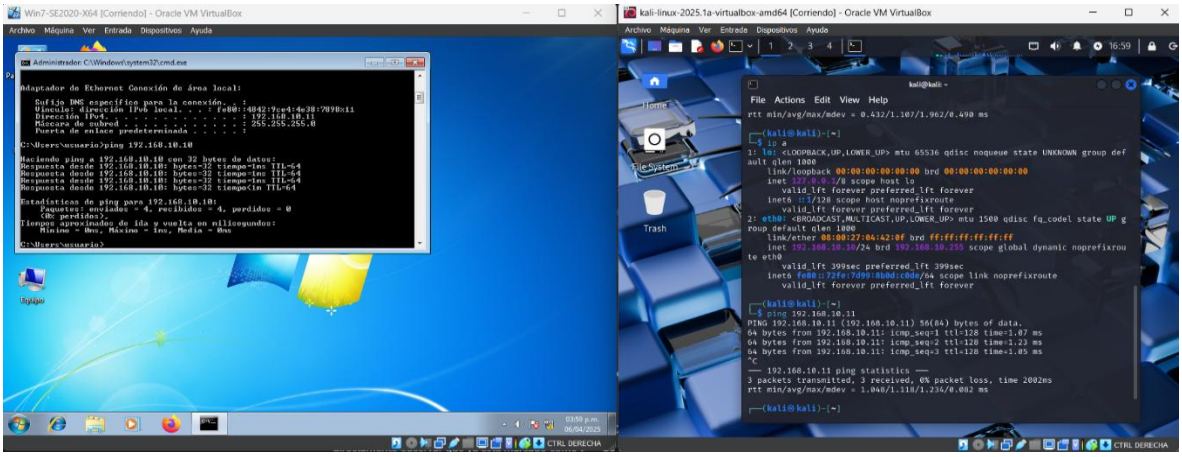
Integración con otras herramientas: Nmap, OpenVAS y Metasploit usan CVEs para sus reportes.

Banco de trabajo

En la figura 1 se evidencia la conexión mediante ping entre la máquina virtual Windows y la máquina virtual Linux.

Figura 1

Asignación de IP a cada máquina virtual y comunicación entre ellas



Fuente: Elaboración propia.

En la figura 2 se evidencia como se encuentran las características de la maquina Kali Linux para el banco de trabajo.

Figura 2

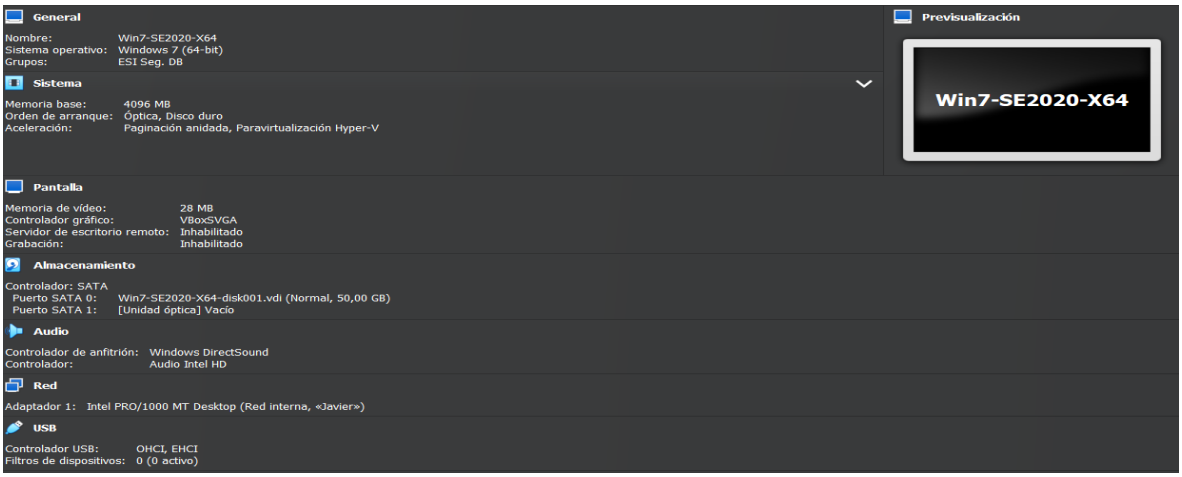
Características del hardware para la maquina Kali Linux

Fuente: Elaboración propia.

En la figura 3 están las características del hardware para el bando de trabajo de la maquina Windows.

Figura 3

Características del hardware para la maquina Windows



Fuente: Elaboración propia.

Etapa 2 Actuación ética y legal.

Análisis referente al acuerdo legal del contrato

El Anexo 3 (Acuerdo) presenta varias cláusulas que son éticamente cuestionables y potencialmente ilegales, especialmente en relación con el Anexo 2 (Escenario 2), donde se menciona que:

El contrato fue redactado por un abogado despedido por procesos ilícitos.

La gerencia no revisó los contratos y advierte suma precaución antes de firmar.

Se incluyen obligaciones de no denunciar actividades ilegales (como espionaje o acceso abusivo a sistemas).

Las cláusulas que se encuentran en el documento que conllevan a obligaciones o prohibiciones que llevaría a cualquier ingeniero el cual acepte este contrato a penar legalmente serian:

Clausula Segunda, Punto 2: Habla sobre la información confidencial que deberá manejar el receptor y trata como confidencial datos secretos como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos. El solo hecho de catalogar esta información como confidencial y no como evidencia de un delito representa una naturalización de actividades ilícitas y una intención de ocultamiento sistemático de conductas que vulneran los derechos fundamentales y el ordenamiento jurídico colombiano.

Cláusula Cuarta, Punto 3 y 4: Obliga al receptor a no denunciar actividades sospechosas de espionaje o procesos ilegales, incluso si involucran apropiación de información de terceros. Esto contradice principios éticos y legales, ya que impide reportar delitos como el acceso

abusivo a sistemas informáticos o interceptación de información, acciones tipificadas como delitos en la Ley 1273 de 2009 de Colombia.

Cláusula Cuarta, Punto 9: Prohíbe divulgar información confidencial o ilegal sin consentimiento de CyberFort Technologies, incluso si dicha información evidencia actos ilícitos. Esto podría encubrir actividades criminales y viola el deber ético de reportar irregularidades.

Cláusula Octava: Exime a CyberFort Technologies de responsabilidad legal y penal si se encuentra información ilegal en poder del receptor, obligando a este a contratar un abogado privado. Esto es abusivo y busca proteger a la empresa de consecuencias legales por sus actos.

Artículos vulnerados de la Ley 1273 de 2009

La Ley 1273 de 2009, que reforma el Código Penal colombiano para proteger la información y los datos, es claramente vulnerada en los siguientes aspectos:

Tabla 1 Artículos vulnerados encontrados en el contrato

Artículo	Descripción	Justificación de vulneración
Artículo 269A	Acceso no autorizado a sistemas informáticos	El acuerdo exige no denunciar accesos abusivos, lo cual favorece este delito.
Artículo 269B	Obstaculización ilegítima de sistemas	Se promueve la no denuncia de estas actividades, lo que posibilita su ocurrencia.

Artículo 269C	Interceptación de datos informáticos	El acuerdo reconoce como “confidencial” datos de interceptaciones, impidiendo su denuncia.
Artículo 269E	Uso de software malicioso	Si durante el proceso se utilizan herramientas ilegales (p. ej. spyware), la cláusula de silencio resulta encubridora.
Artículo 269F	Violación de datos personales.	Si la empresa maneja información personal sin consentimiento, violaría este artículo.

Fuente: Propia.

Analisis sobre propuesta de trabajo en la empresa CyberFort Technologies.

Con conocimiento de lo estipulado en el anexo 3 – Acuerdo. ¿Aplicaría a este trabajo en CyberFort Technologies?

No aplicaría, pese a la oferta de un sueldo elevado y contrato con beneficios por las siguientes razones:

Argumentos:

Tener ética y legalidad: Aceptar el trabajo con base en un acuerdo que exige encubrir delitos informáticos es contrario a mi deber legal y ético como ingeniero.

Estaría violando el Código de Ética del COPNIA (Ley 842 de 2003):

Artículo 31(f): Obliga a denunciar delitos conocidos en el ejercicio profesional. Firmar este acuerdo implicaría incumplir este deber.

Artículo 32(j): Prohíbe recibir beneficios por encubrir actos ilegales.

Artículo 34 (a): Prohíbe Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes

Artículo 39(a): Exige mantener secreto profesional, pero no cubre actividades delictivas.

Tener responsabilidad profesional: Según el COPNIA, el ingeniero debe proteger la sociedad, denunciar irregularidades y actuar con integridad. Esto llegaría a un riesgo Penal donde participar en una organización que oculta actividades ilegales podría convertirme en cómplice, esto podría llevar a sanciones penales y pérdida de la matrícula profesional (Congreso de Colombia, 2003).

Análisis a "Ciberespionaje y Ética en CyberFort Technologies"

Implicaciones Legales y Éticas

El caso de CyberFort Technologies presenta graves violaciones éticas y legales. Desde una perspectiva ética, la empresa incumplió principios fundamentales como la confidencialidad, la integridad y la lealtad hacia su cliente, al acceder y vender información sensible sin autorización. Esto contradice los códigos de conducta profesionales.

Legalmente, estas acciones podrían constituir delitos bajo la Ley 1273 de 2009 de Colombia, que penaliza el acceso no autorizado a sistemas informáticos y la violación de datos personales. Además, el Decreto 1377 de 2013, que reglamenta la protección de datos personales, exige que las empresas manejen la información con estándares de seguridad estrictos, lo que CyberFort incumplió al explotar los datos obtenidos.

Respuestas a Interrogantes

Acceso a información sensible y prevención de explotación indebida:

Las empresas de ciberseguridad deben tener acceso limitado a la información sensible, restringido únicamente a lo necesario para cumplir con la auditoría. Para evitar abusos, se recomienda:

Contratos claros: Incluir cláusulas específicas que delimiten el alcance del acceso y las consecuencias por violaciones.

Principio de mínimo privilegio: Otorgar permisos temporales y revocarlos una vez finalizada la auditoría.

Auditorías internas: Monitorear las actividades de los empleados durante el proceso.

Puntos clave sobre el acceso a información sensible:

Principio de necesidad: El acceso a la información sensible debe limitarse estrictamente a lo que sea necesario para llevar a cabo la auditoría de manera efectiva. Cualquier acceso que vaya más allá de este principio debe evitarse.

Alcance definido: El alcance de la auditoría debe definirse claramente desde el inicio, especificando los sistemas, aplicaciones y tipos de datos que se incluirán en la evaluación. Esto ayuda a delimitar el acceso a la información.

Minimización de datos: Las empresas de ciberseguridad deben esforzarse por acceder a la menor cantidad posible de datos sensibles. En muchos casos, se pueden utilizar datos anonimizados, pseudonimizados o entornos de prueba para realizar ciertas evaluaciones sin necesidad de acceder a datos reales de producción.

Finalidad específica: El acceso a la información sensible debe tener una finalidad específica y legítima relacionada directamente con los objetivos de la auditoría (por ejemplo, identificar vulnerabilidades, evaluar controles de seguridad, analizar registros de actividad).

Consentimiento informado: Los clientes deben estar completamente informados sobre qué tipo de información sensible será accedida, por qué, cómo se utilizará y cómo se protegerá durante y después de la auditoría. Se debe obtener su consentimiento explícito.

Garantías en el acceso para qué de ninguna forma sea explotado:

Para poder garantizar se deben implementar una serie de medidas y consideraciones, enmarcadas dentro de la legislación colombiana y las mejores prácticas internacionales:

1. **Definición Clara del Alcance de la Auditoría:**

Especificidad: El contrato de auditoría debe definir de manera precisa qué sistemas, datos y procesos serán objeto de la revisión. Esto limita el acceso de la empresa de ciberseguridad únicamente a la información relevante para la auditoría.

Justificación: Cualquier solicitud de acceso a información sensible debe estar justificada por los objetivos de la auditoría y ser aprobada por el cliente.

2. **Acuerdos de Confidencialidad Sólidos (NDA):**

Legalmente vinculantes: Se deben establecer acuerdos de confidencialidad robustos que definan claramente las obligaciones de la empresa de ciberseguridad con respecto a la protección de la información del cliente. Estos acuerdos deben incluir cláusulas sobre la no divulgación, el uso exclusivo para los fines de la auditoría y las responsabilidades en caso de incumplimiento.

3. **Principios de Minimización de Datos:**

Acceso limitado: La empresa de ciberseguridad solo debe acceder a la cantidad mínima de datos sensibles necesaria para llevar a cabo la auditoría. Se deben evitar copias innecesarias de la información.

Anonimización y seudonimización: Siempre que sea posible, se deben utilizar técnicas de anonimización o seudonimización para reducir la sensibilidad de los datos analizados.

4. **Controles de Acceso y Seguridad:**

Acceso basado en roles: El acceso a la información sensible dentro de la empresa de ciberseguridad debe estar estrictamente limitado al personal autorizado y necesario para la auditoría.

Autenticación y autorización: Se deben implementar mecanismos robustos de autenticación y autorización para controlar quién accede a qué información y cuándo.

Registro de actividad (logs): Se deben mantener registros detallados de todas las actividades de acceso a la información sensible, incluyendo quién accedió, qué información y cuándo. Estos registros deben ser auditados periódicamente.

Transferencia segura: Cualquier transferencia de información sensible entre el cliente y la empresa de ciberseguridad debe realizarse a través de canales seguros y cifrados.

5. **Obligaciones Contractuales y Legales:**

Responsabilidad contractual: El contrato de auditoría debe establecer claramente la responsabilidad de la empresa de ciberseguridad en caso de una violación de la seguridad de la información.

Ley 1581 de 2012 (Colombia): La Ley de Protección de Datos Personales en Colombia establece principios como la finalidad, la necesidad y la seguridad en el tratamiento de datos personales. Las empresas de ciberseguridad que accedan a datos personales de clientes durante una auditoría están obligadas a cumplir con esta ley y garantizar la confidencialidad y seguridad de dichos datos.

Código de Ética (Ley 842 de 2003): Para los profesionales de la ingeniería que trabajen en empresas de ciberseguridad, el Código de Ética establecido en la Ley 842 de 2003 exige mantener la confidencialidad de la información de sus clientes y actuar con integridad y profesionalismo.

6. **Supervisión y Auditoría:**

Supervisión por el cliente: El cliente debe supervisar de cerca el proceso de auditoría y asegurarse de que la empresa de ciberseguridad cumpla con los términos del contrato y las políticas de seguridad acordadas.

Auditorías a la empresa de ciberseguridad: El cliente puede realizar auditorías a la empresa de ciberseguridad para verificar sus controles de seguridad y el cumplimiento de los acuerdos de confidencialidad.

7. **Selección Rigurosa de la Empresa de Ciberseguridad:**

Reputación y experiencia: Es crucial seleccionar una empresa de ciberseguridad con una sólida reputación, experiencia comprobada y buenas prácticas en el manejo de información sensible.

Certificaciones: Verificar si la empresa cuenta con certificaciones relevantes en seguridad de la información, como la ISO 27001.

Mecanismos de supervisión y control

Implementar mecanismos robustos es crucial en las empresas dedicadas al campo de ciberseguridad para evitar que se usen las de herramientas avanzadas de análisis forense de manera indebida por parte de sus empleados. Estos mecanismos deben abarcar aspectos técnicos, procedimentales y éticos:

1. **Controles de Acceso y Autorización Granulares:**

Acceso basado en roles y necesidad de conocer: El acceso a herramientas de análisis forense debe estar estrictamente limitado a los empleados que las necesiten para sus tareas específicas. Se deben definir roles con permisos específicos para cada herramienta y tipo de análisis.

Autenticación multifactor (MFA): Implementar MFA para acceder a las herramientas y a los sistemas donde se almacenan los datos analizados añade una capa adicional de seguridad.

Listas de control de acceso (ACLs): Configurar ACLs en los sistemas y repositorios de datos para restringir el acceso solo a usuarios y procesos autorizados.

2. **Registro y Auditoría Detallada (Logging):**

Registro exhaustivo de actividad: Se deben mantener registros detallados de cada uso de las herramientas de análisis forense, incluyendo quién accedió, qué herramienta se utilizó, qué datos se analizaron, cuándo se realizó la actividad y cualquier modificación realizada.

Centralización y seguridad de logs: Los registros deben almacenarse de forma centralizada en un sistema seguro e inalterable, protegido contra accesos no autorizados y modificaciones.

Auditoría periódica de logs: Un equipo independiente o un sistema automatizado debe revisar periódicamente los logs para identificar actividades sospechosas, patrones inusuales o accesos no autorizados.

3. **Políticas y Procedimientos Claros:**

Política de uso aceptable de herramientas: Definir una política clara que especifique los usos permitidos y prohibidos de las herramientas de análisis forense, así como las consecuencias de su uso indebido.

Procedimientos operativos estándar (POEs): Establecer POEs detallados para la realización de análisis forense, incluyendo los pasos a seguir, la documentación requerida y las aprobaciones necesarias.

Protocolos de manejo de evidencia digital: Implementar protocolos estrictos para la adquisición, custodia, análisis y disposición de la evidencia digital, garantizando su integridad y cadena de custodia.

Proceso de aprobación para análisis sensibles: Para análisis que involucren información altamente sensible o que puedan tener implicaciones éticas significativas, se debe requerir una aprobación explícita por parte de la gerencia o un comité designado.

4. **Supervisión Técnica y Alertamiento:**

Sistemas de detección de anomalías: Implementar sistemas que monitoreen el uso de las herramientas y generen alertas ante actividades inusuales o que se desvíen de los patrones de uso normales.

Monitorización en tiempo real: En ciertos casos justificados y dentro de los límites legales y de privacidad, se podría considerar la monitorización en tiempo real de las sesiones de uso de las herramientas.

Integración con sistemas SIEM: Integrar los logs de las herramientas de análisis forense con un sistema de gestión de eventos e información de seguridad (SIEM) para una correlación y análisis más amplios.

5. **Controles Humanos y Éticos:**

Selección y contratación rigurosa: Realizar verificaciones exhaustivas de antecedentes y referencias de los candidatos a empleados que tendrán acceso a estas herramientas.

Capacitación y concienciación continua: Proporcionar capacitación regular sobre el uso ético y responsable de las herramientas de análisis forense, así como sobre las políticas de la empresa y las implicaciones legales del uso indebido.

Código de conducta y ética profesional: Reforzar un código de conducta claro que enfatice la integridad, la confidencialidad y el respeto por la privacidad de la información.

Acuerdos de confidencialidad y no divulgación: Exigir la firma de acuerdos de confidencialidad y no divulgación que aborden específicamente el manejo de la información sensible y el uso de las herramientas forenses.

Evaluaciones de desempeño y revisiones éticas: Incorporar en las evaluaciones de desempeño la conducta ética y el cumplimiento de las políticas de seguridad. Realizar revisiones éticas periódicas sobre el uso de las herramientas.

Canales de denuncia confidenciales: Establecer canales seguros y confidenciales para que los empleados puedan reportar sospechas de uso indebido sin temor a represalias.

6. **Auditorías Internas y Externas:**

Auditorías técnicas: Realizar auditorías técnicas periódicas para verificar la configuración y el cumplimiento de los controles de acceso, el registro de actividad y la seguridad de los sistemas.

Auditorías de cumplimiento: Llevar a cabo auditorías de cumplimiento para asegurar que se están siguiendo las políticas y los procedimientos establecidos.

Auditorías éticas: Considerar la realización de auditorías éticas para evaluar la cultura de la empresa y la comprensión de los principios éticos en el uso de las herramientas.

3. **Reglas adecuadas para asegurar que no ocurra nuevamente y restaurar la confianza.**

Cuando una empresa contratista en ciberseguridad comete actos de ciberespionaje, como en el caso de CyberFort Technologies, las autoridades estatales tienen la obligación de actuar con contundencia, para proteger la seguridad nacional, restaurar la confianza pública y evitar precedentes peligrosos.

Acciones legales y contractuales inmediatas

Rescisión del contrato y sanción económica:

Se debe aplicar la cláusula de resolución anticipada del contrato por incumplimiento grave.

Imposición de cláusulas penales o demandas por perjuicios si están contempladas.

Denuncia penal formal ante la Fiscalía General de la Nación:

Los responsables deben ser procesados por delitos tipificados en la Ley 1273 de 2009. (acceso abusivo, interceptación, violación de datos, etc.) y el Código Penal Colombiano.

Colaboración internacional:

Si hay implicaciones con otros Estados por ejemplo, si la información fue vendida a empresas extranjeras, se deben activar mecanismos de cooperación judicial internacional a través de INTERPOL.

Medidas para restaurar la confianza institucional

Auditoría independiente postincidente:

Contratar una firma neutral y certificada para revisar los accesos, detectar vulnerabilidades y determinar el alcance del daño.

Informe público controlado:

Comunicar de manera oficial y responsable los hechos a los ciudadanos y al Congreso, sin revelar detalles sensibles, como parte de una política de transparencia institucional.

Revisión del marco contractual de servicios de ciberseguridad:

Incluir criterios éticos, cláusulas anticorrupción, compromisos de responsabilidad civil y penal, e implementación obligatoria de ISO/IEC 27001 y 27701.

Certificación y vigilancia de empresas contratistas:

Crear un registro nacional de empresas de ciberseguridad confiables, evaluadas por el Estado, similar al RUES (Registro Único Empresarial).

Fortalecimiento normativo y políticas públicas

Actualización del marco legal colombiano:

Aunque Colombia cuenta con leyes como la Ley 1273 de 2009 y la Ley 1581 de 2012, aún no existe una regulación específica para empresas privadas de ciberseguridad. Es urgente legislar sobre la responsabilidad empresarial en manejo de datos clasificados, el licenciamiento profesional obligatorio para auditores forenses y la regulación de exportación/importación de software de monitoreo avanzado.

Creación de una Agencia Nacional de Ciberseguridad:

Similar al modelo español (INCIBE) o estadounidense (CISA), encargada de supervisar empresas del sector, emitir alertas y lineamientos e investigar fraudes tecnológicos.

Cooperación internacional y listas negras

Incluir empresas sancionadas en listas negras: Impedir que empresas implicadas en ciberespionaje puedan ser contratadas nuevamente por entidades públicas o privadas en Colombia.

Participación en alianzas regionales:

Colombia puede fortalecer sus pertenencias al Grupo de Acción de Ciberseguridad de la OEA , para compartir alertas de riesgo y establecer estándares mínimos de contratación internacional.

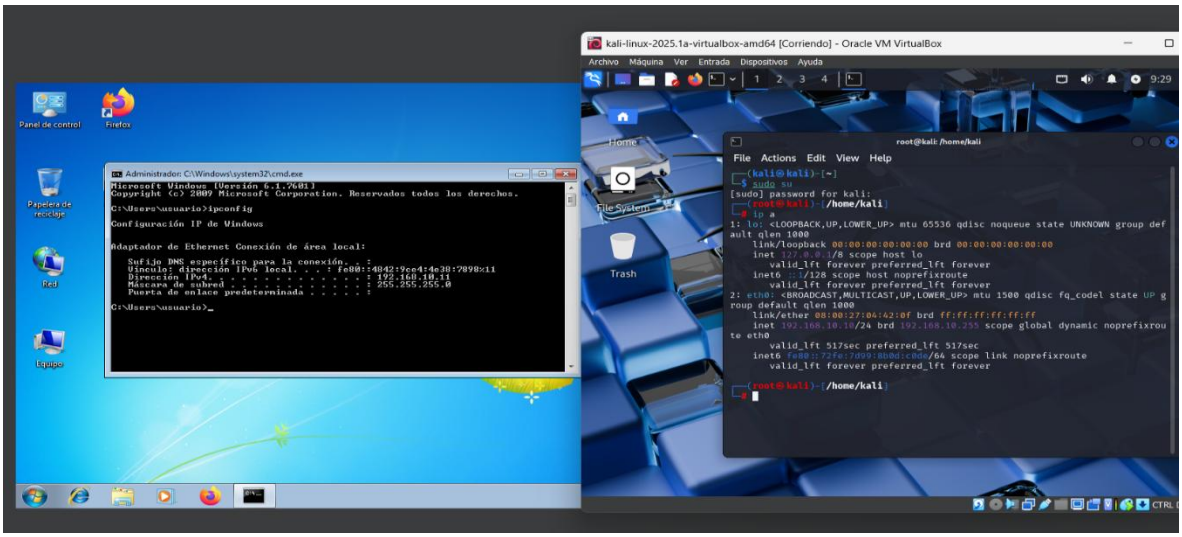
Etapa 3 ejecución de pruebas de intrusión.

Descripción de las herramientas utilizadas en equipos Redteam

Se descargan dos máquinas virtuales, una Kali Linux y una Windows suministradas por el tutor, para este escenario se configuran las maquinas en una red interna con el fin de facilitar la comunicación entre estas. La red le da a la maquina Linux la IP 192.168.10.10 mientras que a la maquina Windows la 192.168.10.11, se comprueba esto mediante comandos, para la maquina Linux se ingresa en la terminal de comandos, se sube los privilegios con el comando Sudo su y se verifica la información de la IP con el comando ip address. Por otra parte, para la maquina Windows se ingresa al CMD y se ingresa el comando ipconfig, este dando la información de la red.

Figura 4

Escenario virtualizado



Fuente: Elaboración propia.

3.2 Verificación de conectividad entre las máquinas virtuales

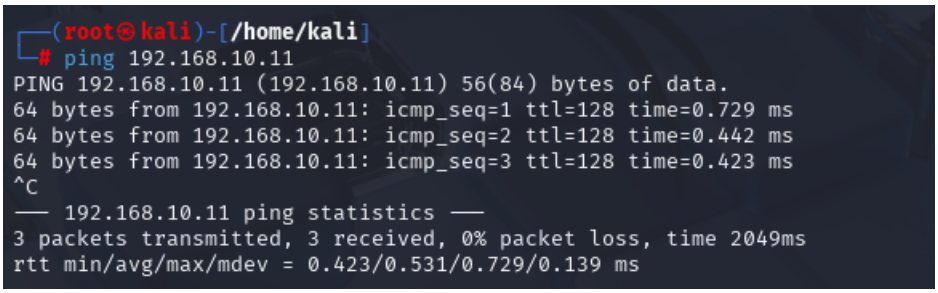
Antes de iniciar cualquier proceso de reconocimiento o análisis, se procedió a comprobar la conectividad de red entre las máquinas virtuales del entorno de pruebas. La máquina atacante (Kali Linux) debía ser capaz de comunicarse con la máquina objetivo (Windows 7), por lo cual se utilizó el comando ping para validar dicha conexión.

ping 192.168.10.11 Envía paquetes ICMP ("echo request") al objetivo para comprobar si está activo y accesible desde la máquina atacante.

La respuesta positiva indicó que ambas máquinas se encontraban correctamente configuradas dentro de la misma red virtual, permitiendo continuar con el proceso de evaluación de seguridad.

Figura 5

Ping a la maquina Windows



Fuente: Elaboración propia.

3.3 Datos e información relevante suministrada por el anexo 4 escenario 3 para identificar el fallo de seguridad

Sistema operativo identificado: Windows

El anexo especifica que la máquina con fuga de información corre bajo un sistema operativo Windows. Esto orienta la búsqueda hacia vulnerabilidades conocidas en versiones antiguas de Windows, como Windows 7 o Server 2008.

Presencia de una aplicación vulnerable con exploit conocido

Se menciona explícitamente que existe una aplicación vulnerable instalada que puede estar asociada a un exploit que permite abrir una shell, escalar privilegios, o ejecutar otros tipos de ataque. Esto sugiere una vulnerabilidad crítica explotable remotamente.

Investigación de escalamiento de privilegios mediante usuario administrador

Se menciona que parte de la investigación forense busca evidencia de un usuario tipo administrador creado por medios ilegítimos, lo cual es un síntoma típico de explotación post-compromiso tras una ejecución remota.

3.4 Pasos de un Pentesting

Reconocimiento activo mediante la herramienta Nmap

La fase de reconocimiento permite identificar qué servicios y puertos están disponibles en la máquina objetivo. Para ello se utilizó la herramienta nmap, una de las más completas para escaneo de red, con las opciones para escaneo SYN, detección de versiones y sistema operativo. (Nmap Project, 2023)

nmap -sS -sV -O 192.168.10.11

-sS: Realiza un escaneo SYN (también llamado escaneo furtivo o "half-open"), ideal para evitar la detección por firewalls.

-sV: Detecta versiones de servicios que corren en los puertos abiertos.

-O: Intenta identificar el sistema operativo del host objetivo mediante fingerprinting TCP/IP.

Este comando reveló información crítica:

Puertos abiertos: 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), entre otros.

Servicios activos: Microsoft SMB, HTTPAPI.

Sistema operativo estimado: Windows 7 / Server 2008 R2

La presencia del puerto 445 abierto junto con la identificación de SMB indicó una superficie de ataque potencial para vulnerabilidades conocidas.

Figura 6

Comando nmap

Fuente: Elaboración propia.

Enumeración del sistema mediante la herramienta Enum4linux

Para obtener información detallada del sistema Windows, se empleó la herramienta enum4linux, que permite realizar enumeración a través de SMB sin necesidad de credenciales.

enum4linux -a 192.168.10.11

Enum4linux es una herramienta especializada en la enumeración de sistemas Windows a través del protocolo SMB. Puede listar usuarios, grupos, shares, y más. (Kali Linux, 2025). -a: Realiza todas las pruebas posibles (equivale a usar todas las opciones combinadas).

El escaneo reveló:

Nombre del host: PC202006

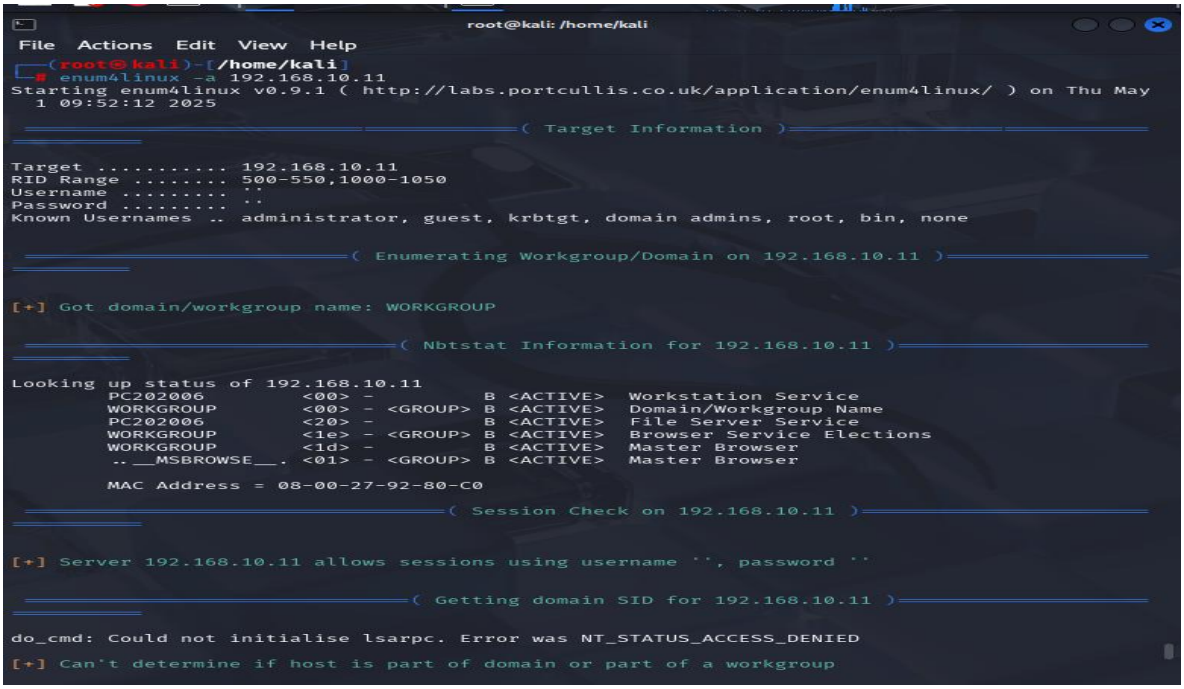
Grupo de trabajo: WORKGROUP

Respuesta activa del servicio NetBIOS y SMB

Estos datos confirmaron la exposición del servicio SMBv1, lo que respaldó la hipótesis de una vulnerabilidad tipo MS17-010.

Figura 7

Comando enum4linux



Fuente: Elaboración propia.

Identificación de la vulnerabilidad MS17-010 (EternalBlue)

El conjunto de datos recogidos en las fases anteriores orientó el análisis hacia una vulnerabilidad específica. La presencia del puerto 445, el sistema Windows 7, y el SMBv1 activo sin parches, sugerían que la máquina podía ser vulnerable a MS17-010, también conocida como EternalBlue.

MS17-010 es una vulnerabilidad crítica de ejecución remota que permite a un atacante ejecutar código arbitrario en el sistema sin autenticación previa, aprovechando una mala gestión de paquetes en SMBv1 buscando en la base de datos de CVE se relacionó la vulnerabilidad CVE-2017-0144. (The MITRE Corporation, 2017)

Explotación mediante la herramienta Metasploit

Se procedió a la explotación de la vulnerabilidad utilizando el framework Metasploit. A través del módulo ms17_010_eternalblue, se configuraron los parámetros necesarios para lanzar el ataque de la siguiente manera.

msfconsole: Inicia el framework Metasploit.

search ms17_010: Busca módulos relacionados con esa vulnerabilidad.

use exploit/windows/smb/ms17_010_eternalblue: Carga el módulo de EternalBlue.

set RHOSTS: IP del objetivo.

set LHOST: IP del atacante (Kali).

set PAYLOAD: Define el tipo de payload que se enviará. Aquí es una reverse shell de tipo Meterpreter.

run: Lanza el ataque.

El resultado fue exitoso: se obtuvo una sesión remota tipo meterpreter, lo cual confirmó que el sistema era vulnerable y que el exploit había logrado inyectar código de forma remota.

Figura 8

Herramienta Metasploit

Fuente: Elaboración propia.

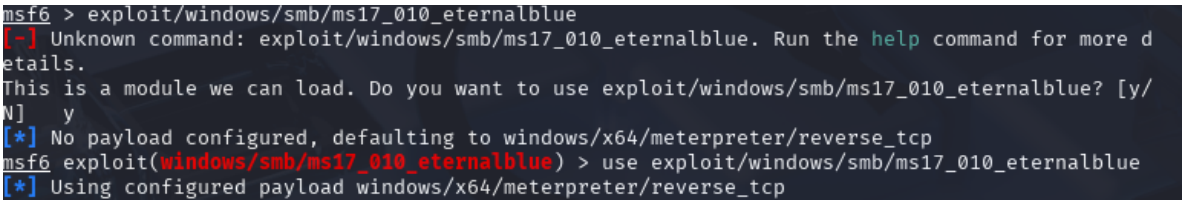
Figura 9

Comando search ms17_010

Fuente: Elaboración propia.

Figura 10

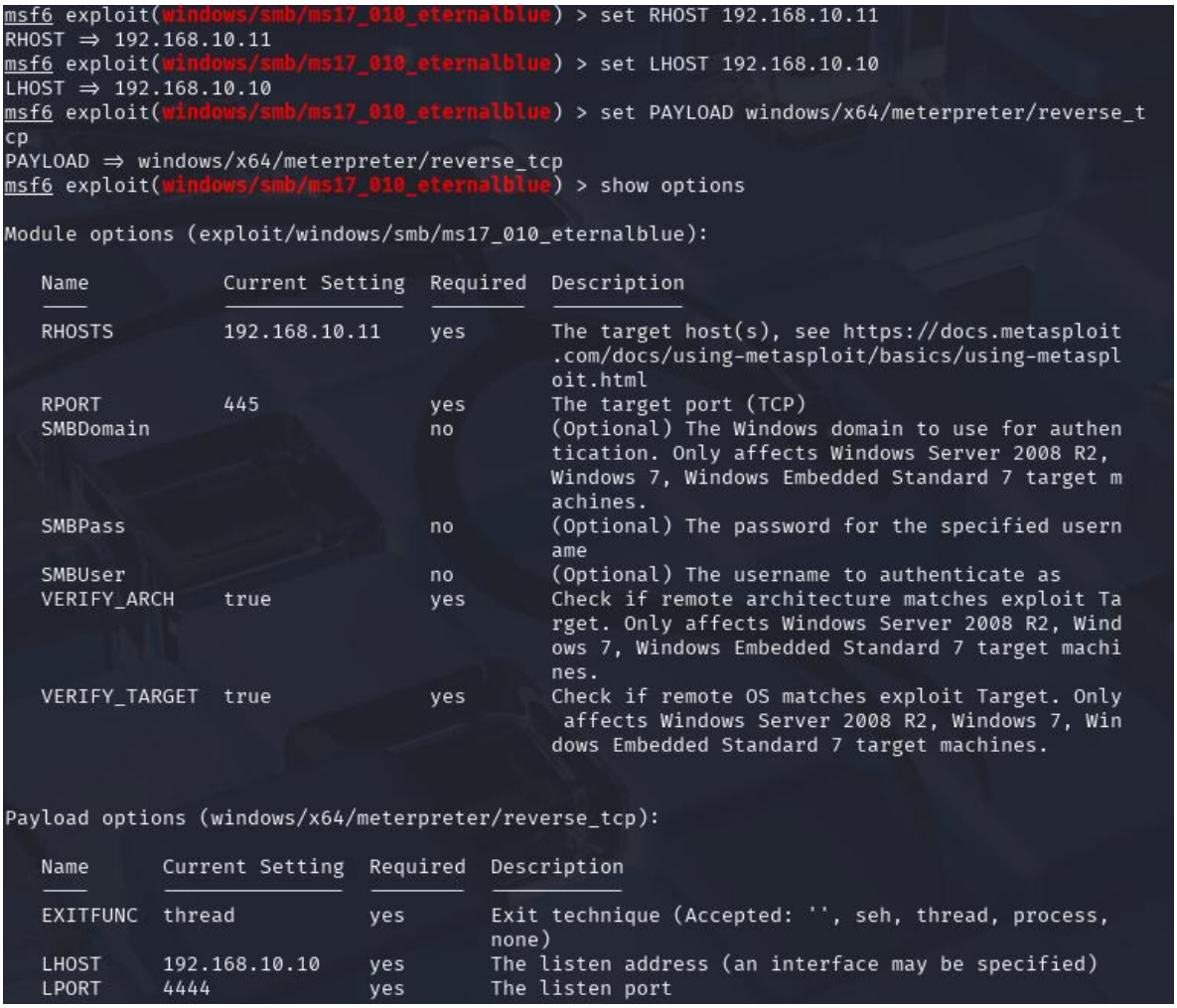
Comando exploit



Fuente: Elaboración propia.

Figura 11

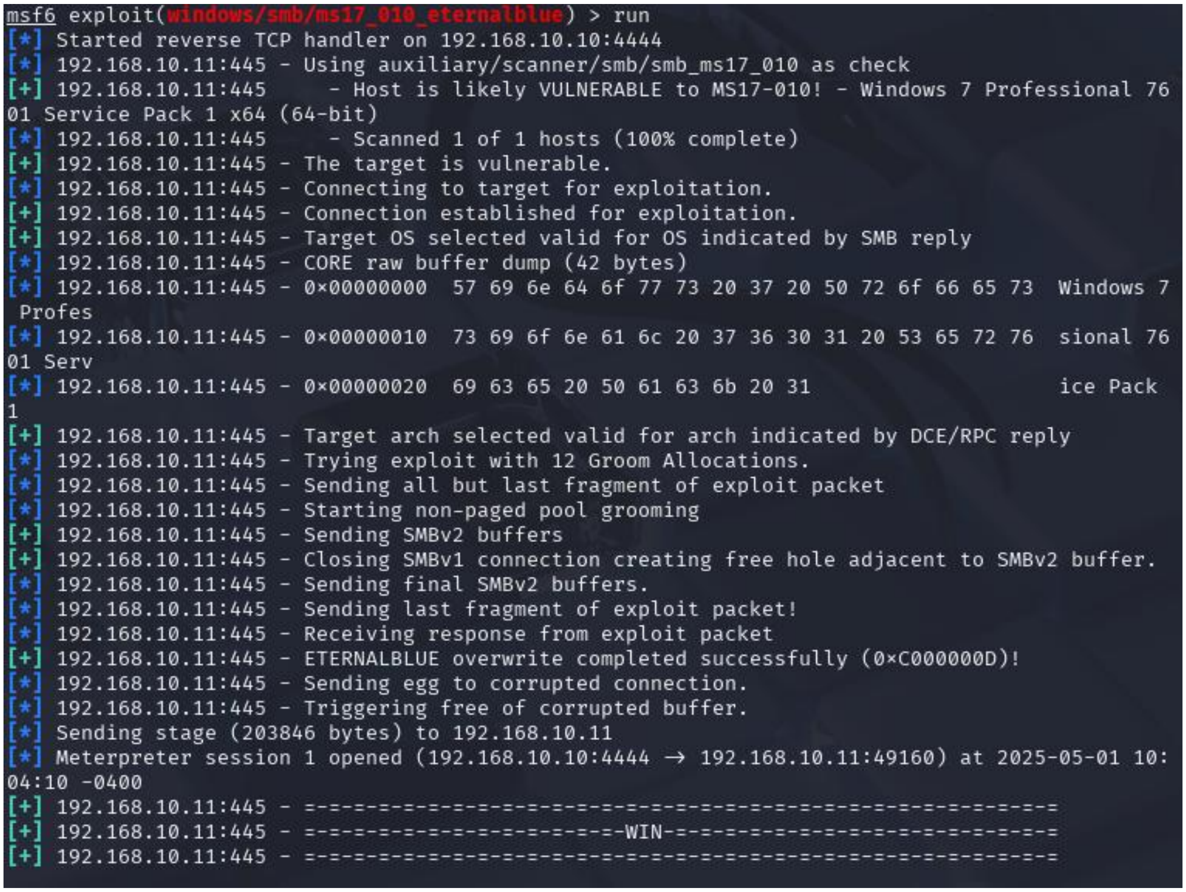
Comandos set y show options



Fuente: Elaboración propia.

Figura 12

Se corre el exploit



Fuente: Elaboración propia.

Post-explotación: Escalación y creación de usuario PoC mediante la herramienta Meterpreter

Desde la sesión meterpreter, se procedió a escalar privilegios y a crear un usuario con privilegios de administrador como prueba de concepto (PoC):

getuid. Este comando se utiliza dentro de una sesión Meterpreter para mostrar el usuario actual bajo el cual se están ejecutando los comandos en el sistema comprometido.

Esto confirma si el exploit se ejecutó con éxito con privilegios elevados. En el contexto de MS17-010, normalmente se obtiene acceso con nivel SYSTEM, el más alto privilegio en Windows.

getsystem. Intenta escalar privilegios automáticamente al nivel SYSTEM.

shell. Abre una shell del sistema dentro de la sesión meterpreter.

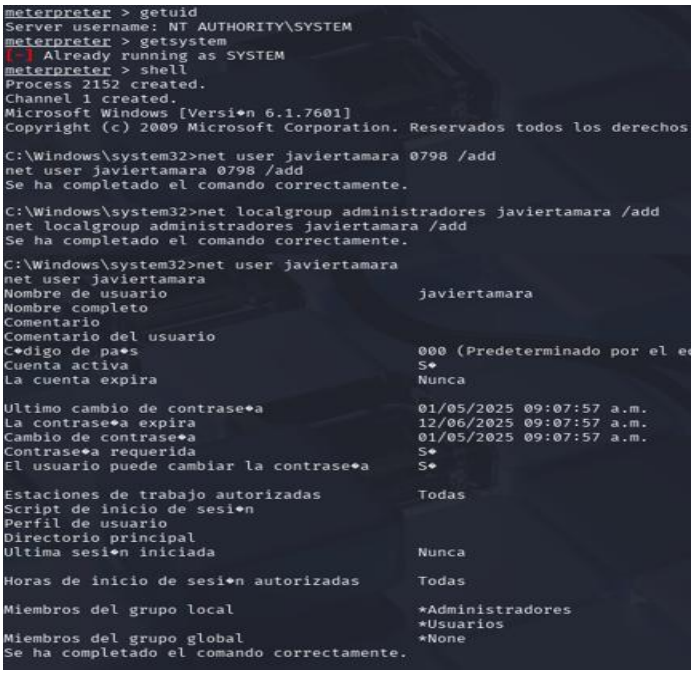
net user javiertamara kali2025 /add. Crea un nuevo usuario local.

net localgroup administradores javiertamara /add. Añade ese usuario al grupo de administradores.

Esto demostró que el atacante tenía el control completo del sistema comprometido.

Figura 13

Creación de usuario

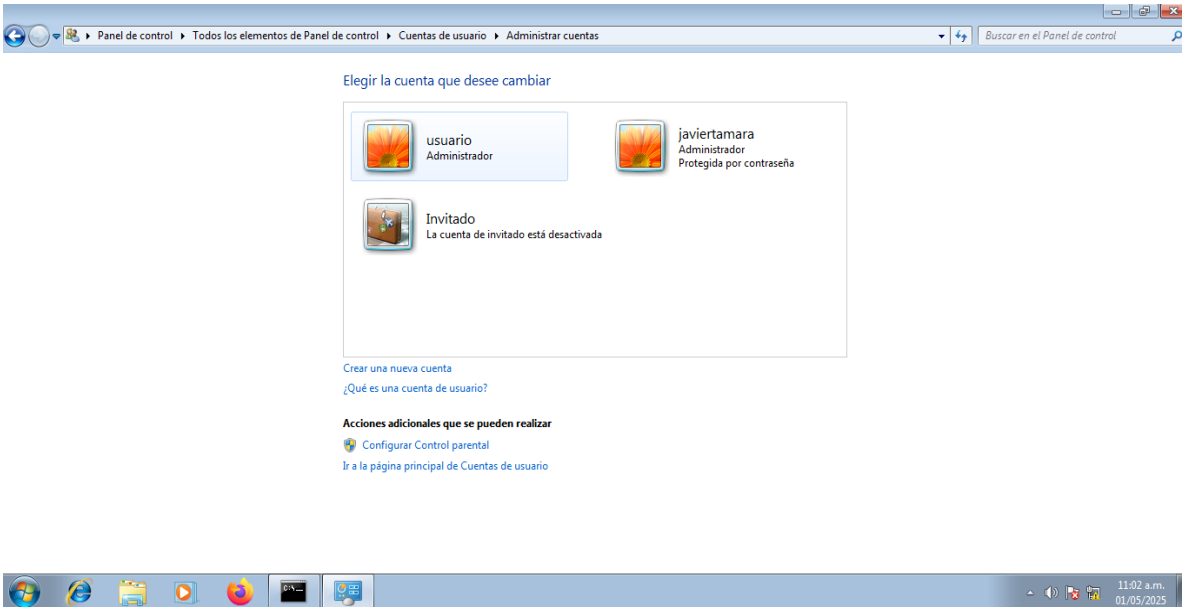


Fuente: Elaboración propia.

Por último, se verifica que el usuario fuese creado de manera correcta en la maquina Windows con el fin de ver que todo el laboratorio fue realizado de manera correcta.

Figura 14

Usuario creado en Windows



Fuente: Elaboración propia.

3.5 ¿Cómo afecta el ataque a la máquina Windows?

El ataque se basa en la explotación de una vulnerabilidad crítica en el servicio SMBv1, presente en sistemas Windows antiguos como Windows 7. Esta falla, conocida como MS17-010 (EternalBlue), permite al atacante ejecutar código malicioso en la máquina vulnerable sin necesidad de autenticación.

Impacto específico del ataque:

Acceso remoto total sin credenciales:

El atacante puede acceder remotamente al sistema sin conocer usuario ni contraseña.

Esto se logra enviando paquetes especialmente diseñados al puerto 445/tcp, que está expuesto.

Ejecución de código con privilegios elevados:

Una vez explotada la vulnerabilidad, el atacante obtiene acceso al sistema con los privilegios más altos (SYSTEM), lo que equivale al control absoluto del equipo.

Instalación de puertas traseras o shells persistentes:

Mediante el payload (en este caso meterpreter), se puede abrir una conexión inversa (reverse shell) para mantener acceso al sistema de forma oculta.

Escalamiento de privilegios y creación de usuarios:

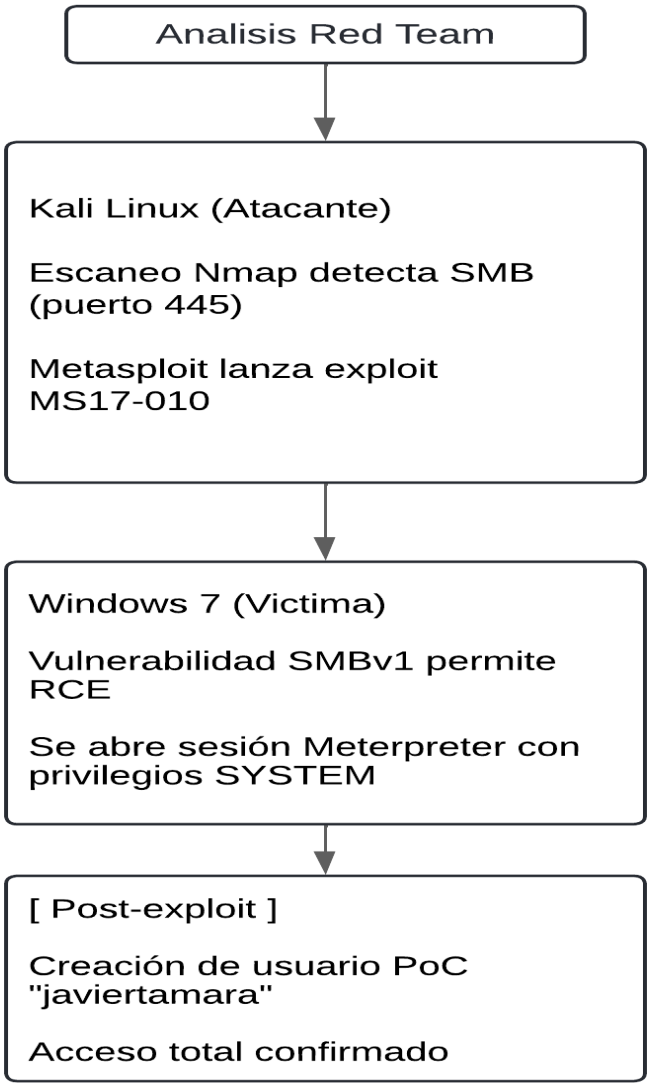
Desde la sesión remota, el atacante puede crear usuarios con derechos de administrador, como se hizo en la prueba de concepto (javiertamara). Esto permite que el atacante regrese al sistema sin explotar nuevamente la vulnerabilidad.

3.6 Representación del ataque

El siguiente esquema ilustra el flujo del ataque llevado a cabo:

Figura 15

Análisis Red Team



Fuente: Elaboración propia.

Etapa 4 Contencion de ataques informáticos

4.1 Acciones a tomar cuando sucede un ataque

Frente a un incidente activo, es fundamental evitar reacciones impulsivas y aplicar una metodología técnica sistemática de contención, preservación de evidencia y análisis inmediato, como lo recomienda el marco NIST SP 800-61r2 para la gestión de incidentes informáticos (NIST, 2012), así como las buenas prácticas sugeridas por ENISA (2021) y FIRST (2020).

Aislar la maquina comprometida

La primera acción para contener el ataque seria aislar la máquina afectada, sin apagarla para evitar la propagación del ataque hacia otras máquinas, la fuga de información hacia el exterior y la destrucción o cifrado de evidencia por parte del atacante.

Esto puede hacerse técnicamente de manera inmediata ejecutando el comando:

netsh interface set interface "Ethernet" admin=disable

es una instrucción de la línea de comandos de Windows que se utiliza para deshabilitar una interfaz de red específica.

Desglose técnico:

netsh: Es una utilidad de línea de comandos que permite configurar y mostrar el estado de varias funciones de red del sistema operativo.

interface: Especifica que la acción a realizar está relacionada con las interfaces de red.

set interface: Indica que se va a modificar la configuración de una interfaz.

"Ethernet": Es el nombre de la interfaz de red que se va a configurar. Este nombre puede variar dependiendo del sistema.

admin=disable: Este parámetro establece el estado administrativo de la interfaz especificada a "deshabilitado". Esto significa que la interfaz se desactivará lógicamente, impidiendo toda comunicación de red a través de ella.

O bien desconectando el cable de red o deshabilitando el adaptador desde el administrador de dispositivos, sin apagar el sistema.

Al desconectar la red, pero mantener la máquina encendida, preservamos la memoria volátil (RAM), las conexiones activas y los procesos maliciosos residentes, que son esenciales para un análisis forense posterior

Recolectar la memoria RAM (antes de reiniciar o apagar)

La siguiente acción es realizar una captura forense de la memoria RAM utilizando herramientas de licencia GPL con WinPMEMo bien Belkasoft RAM Capturer (aunque freeware, puede usarse si se aprueba por la política organizacional).

Esto es fundamental para analizar procesos activos, cadenas de ejecución, cargas maliciosas en memoria (malware fileless) y credenciales temporales almacenadas en texto claro.

Muchos ataques actuales utilizan técnicas fileless que no dejan rastros en disco, por lo tanto, solo pueden analizarse desde una imagen de memoria (Volatility Foundation, 2023).

Verificar conexiones de red activas (indicadores de C2 o exfiltración)

Antes de que se pierda la visibilidad del tráfico en tiempo real, es clave capturar las conexiones activas, por medio del comando en powershell

netstat -ano

Desglose técnico del comando:

netstat: Es el comando principal que muestra las estadísticas de red.

-a: Muestra todas las conexiones y los puertos de escucha. Por defecto, netstat solo muestra las conexiones activas. Esta opción asegura que se listen todos los puertos en estado de escucha, lo cual es crucial para identificar servicios que podrían ser vulnerables o estar comprometidos.

-n: Muestra todas las direcciones y todos los números de puerto en formato numérico. Esto evita que netstat intente resolver los nombres de dominio, lo que puede ralentizar la salida y también es preferible para el análisis automatizado.

-o: Muestra el identificador de proceso (PID) asociado con cada conexión. Esta es una característica muy importante porque permite identificar qué proceso específico está utilizando una conexión o un puerto, lo cual es esencial para detectar procesos maliciosos.

o herramientas como TCPView (Sysinternals) o Wireshark para analizar sesiones con IPs externas, conexiones persistentes, o tráfico cifrado fuera de los canales regulares (HTTPs en puertos no estándar, por ejemplo).

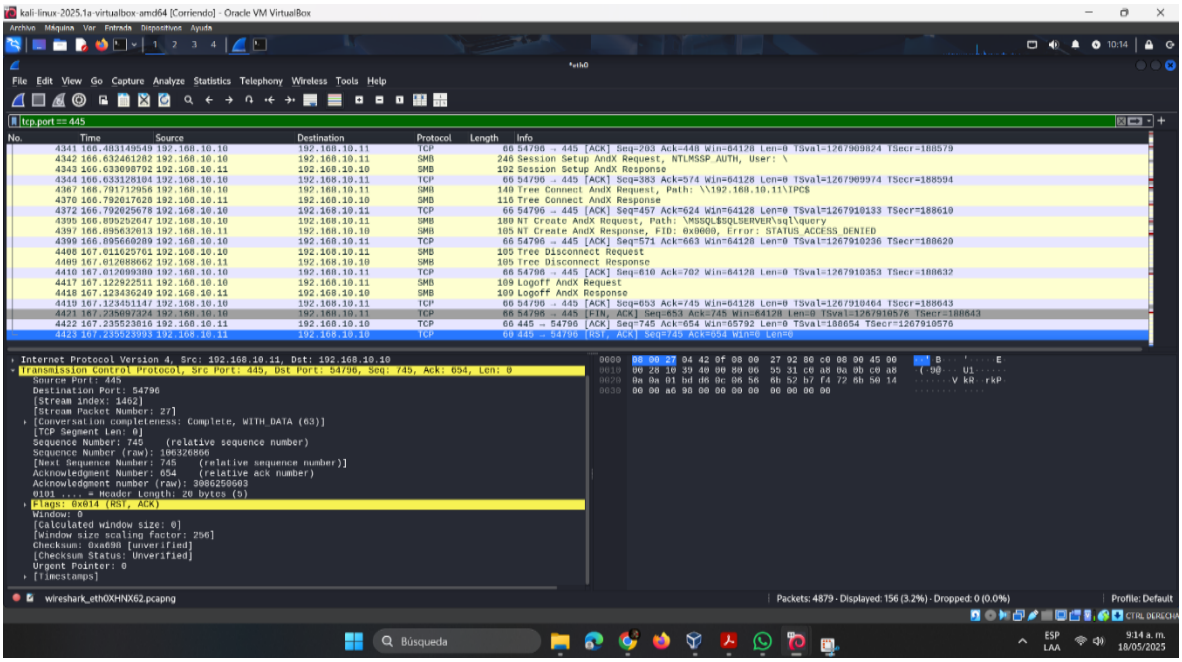
Identificar sesiones activas podría revelar comunicaciones con un servidor C2, exfiltración de datos o presencia de *reverse shells* (MITRE ATT&CK T1071.001).

Como se evidencia en la ilustración 1, la herramienta Wireshark estuvo recolectando información de la red cuando el atacante estaba ingresando al PC Windows. Se obtuvo

información relevante de que era lo que intentaba realizar el atacante y todos se grafica todo el movimiento de información que se mantuvo en el periodo del ataque.

Figura 16

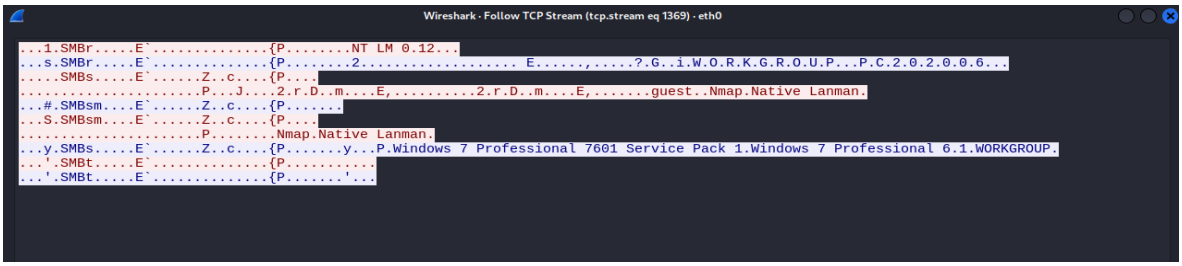
Uso de la herramienta Wireshark



Fuente: Elaboración Propia.

Figura 17

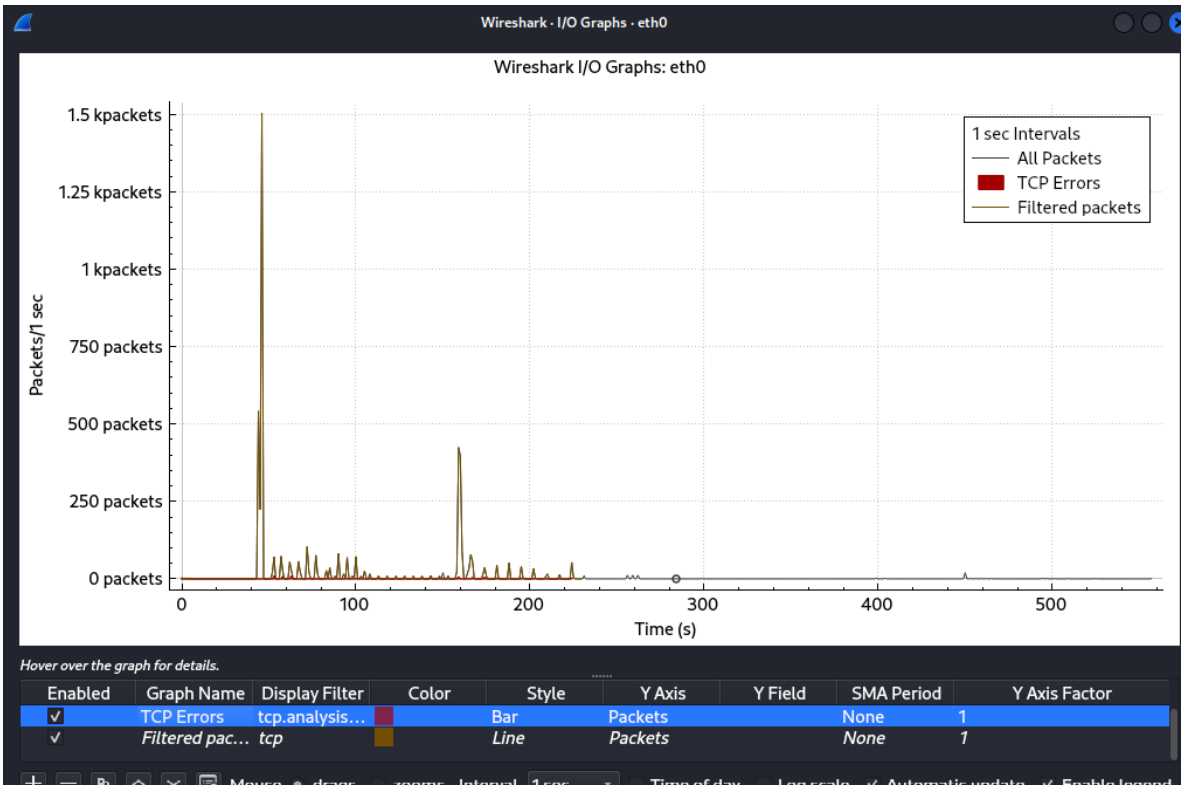
Información relevante de lo que intentaba hacer el atacante



Fuente: Elaboración Propia.

Figura 18

Datos de todos los paquetes en el ataque



Fuente: Elaboración Propia.

Iniciar la recolección de logs del sistema

Paralelamente, se debe comenzar la recolección de Logs del visor de eventos de Windows (eventvwr.msc), eventos de seguridad, sistema y aplicaciones, y registros de inicios de sesión, actividad de PowerShell, tareas programadas sospechosas, etc.

Herramientas recomendadas (todas gratuitas o GPL):

Chainsaw para análisis rápido de logs.

LogonTracer para identificar movimientos laterales o intentos de escalamiento de privilegios.

Sysmon (si estaba preinstalado).

Correlacionar eventos puede permitir reconstruir el punto de entrada del ataque, detectar persistencia o anomalías, y establecer la línea temporal del incidente (NIST SP 800-92).

Evaluar integridad del sistema y posibles persistencias

Se debe buscar técnicas de persistencia comunes:

Revisar el registro en:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Es una clave del Registro de Windows que contiene una lista de programas que se ejecutan automáticamente cada vez que un usuario inicia sesión en el sistema.

Desglose técnico:

HKLM: Significa "HKEY_LOCAL_MACHINE". Esta rama del Registro almacena configuraciones específicas del equipo local, aplicables a todos los usuarios.

Software: Dentro de HKLM, esta subclave contiene configuraciones de software instalado en el equipo.

Microsoft: Esta subclave almacena configuraciones para el software de Microsoft, incluyendo el sistema operativo Windows.

Windows: Contiene configuraciones específicas del sistema operativo Windows.

CurrentVersion: Esta subclave identifica la versión actual de Windows en uso.

Run: Esta es la clave específica que nos interesa. Contiene entradas que representan aplicaciones y comandos que el sistema operativo ejecuta durante el inicio de sesión de un usuario.

- Revisar servicios y tareas programadas maliciosas.

- Analizar qué usuarios están activos y si se han creado nuevos usuarios tipo administrador (como el `javiertamara` usado en el escenario Red Team).

Comandos en cmd como:

net user

net localgroup administrators

son claves para identificar alteraciones.

Las técnicas post-explotación muchas veces incluyen escalamiento de privilegios y persistencia. Detectarlas rápidamente permite cerrar puertas traseras activas. Desde la perspectiva de un Blue Team, como se describe en el "Anexo 5 - Escenario 4.pdf", estos comandos son herramientas importantes para la investigación y la respuesta a incidentes. Se usa net user para identificar cuentas desconocidas o sospechosas y net localgroup administrators para verificar si se han agregado usuarios no autorizados al grupo de administradores.

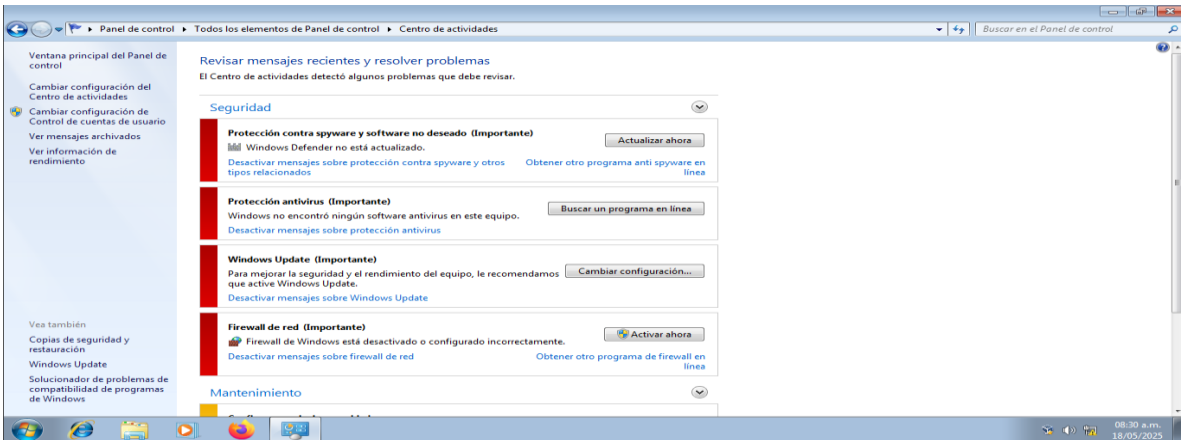
4.2 Medidas de Hardening

Paso 1 Revisar en el panel de control el Centro de actividades

Como se evidencia en la ilustración 4, el centro de actividades nos indica que hay muchas señales en rojo, esto demostrando muchos problemas en la seguridad del equipo.

Figura 19

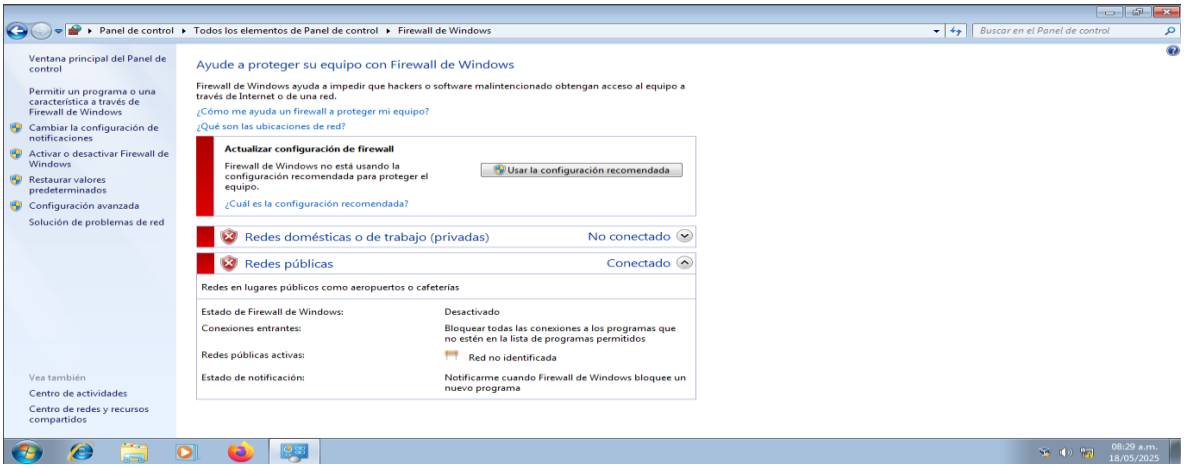
Centro de actividades con muchas señales de problemas



Fuente: Elaboración Propia.

Figura 20

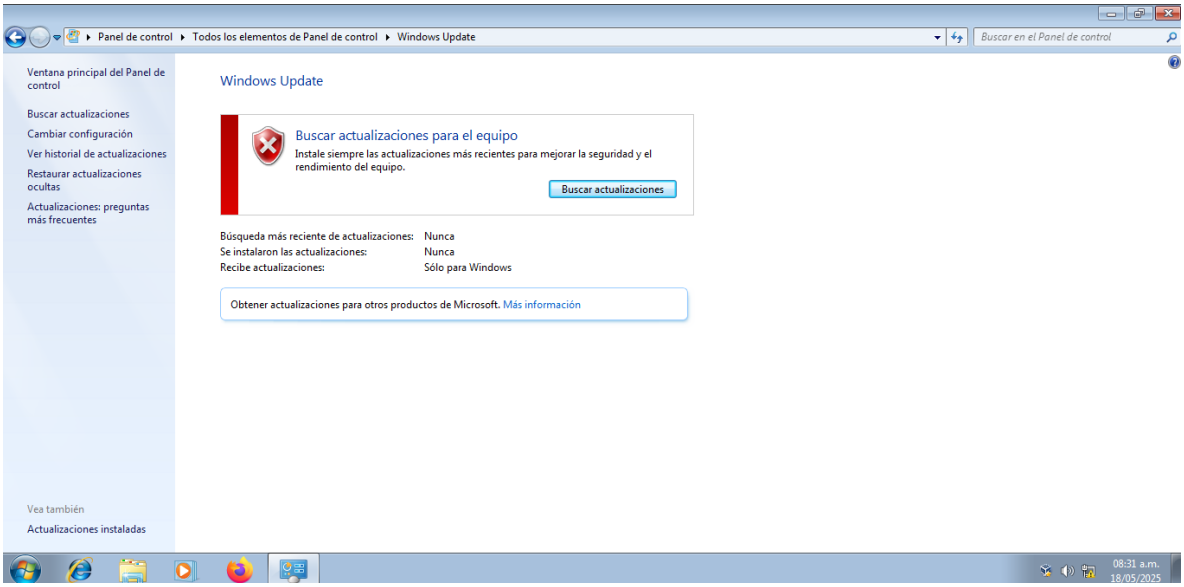
Firewall en estado Desactivado



Fuente: Elaboración Propia.

Figura 21

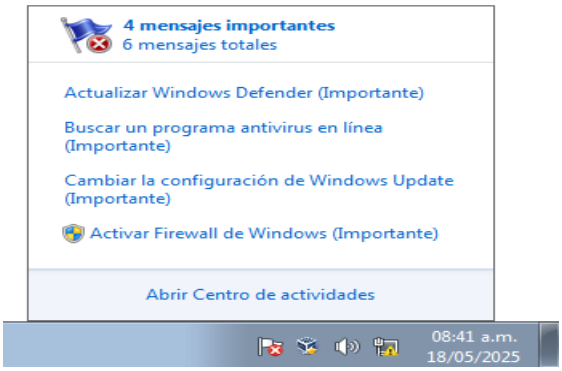
Windows Update nunca actualizado



Fuente: Elaboración Propia.

Figura 22

Centro de actividades mostrando los mensajes importantes

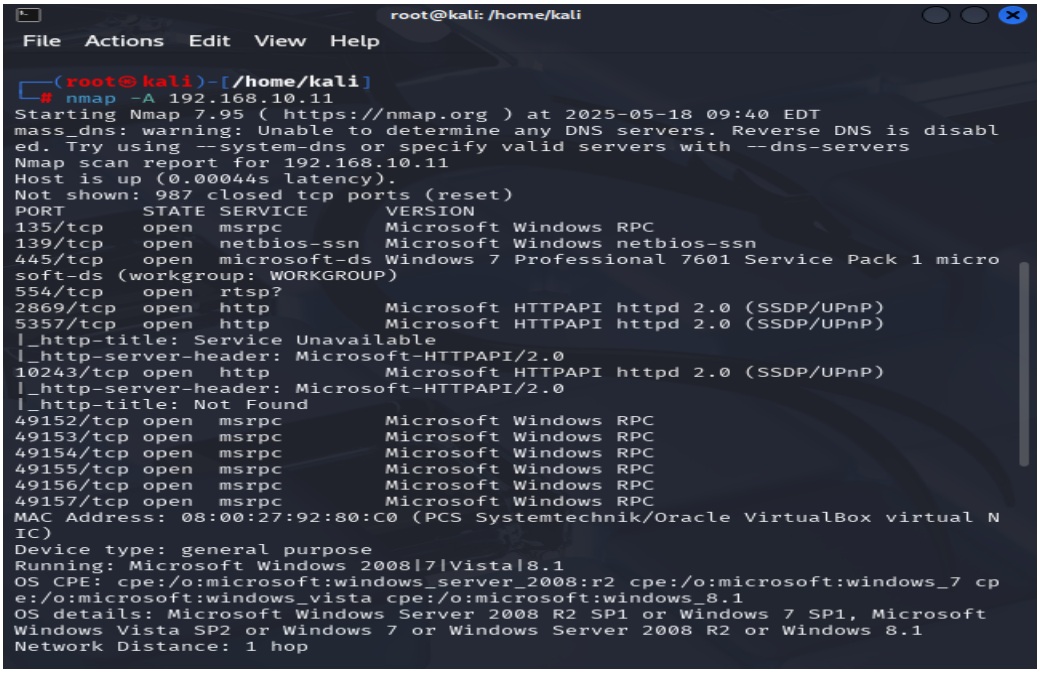


Fuente: Elaboración Propia.

Se comprueba que el PC Windows tiene problemas con la seguridad, ya que con un equipo Linux se puede hacer escaneo de puertos y servicios sin inconveniente como se ilustra en la imagen 8.

Figura 23

Herramienta nmap escaneando



Fuente: Elaboración Propia.

4.3 Paso 2 implementación de las medidas de hardening

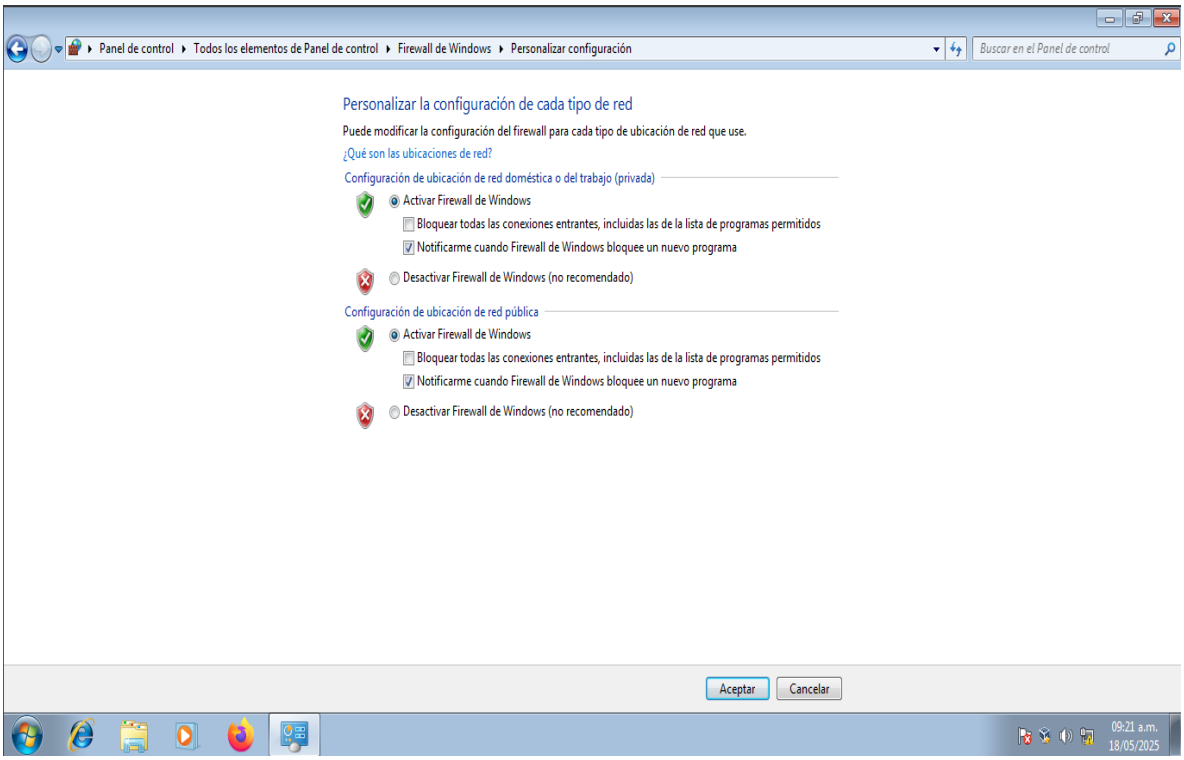
En este caso lo más recomendable seria actualizar o migrar el sistema operativo. La medida más urgente es reemplazar Windows 7, un sistema fuera de soporte desde enero de 2020, por una versión moderna y soportada (ej. Windows 10/11 LTSC o Windows Server 2019/2022).

El exploit EternalBlue (CVE-2017-0144) explota SMBv1 sin parches. La simple instalación de las actualizaciones de seguridad posteriores a marzo de 2017 bloquea este vector de ataque (Microsoft, 2017).

Si por razones operativas no se puede migrar de inmediato, deben aplicarse todos los parches críticos, en particular el boletín de seguridad MS17-010, que corrige la vulnerabilidad explotada y modificar las advertencias que nos mostraba el Centro de actividades.

Figura 24

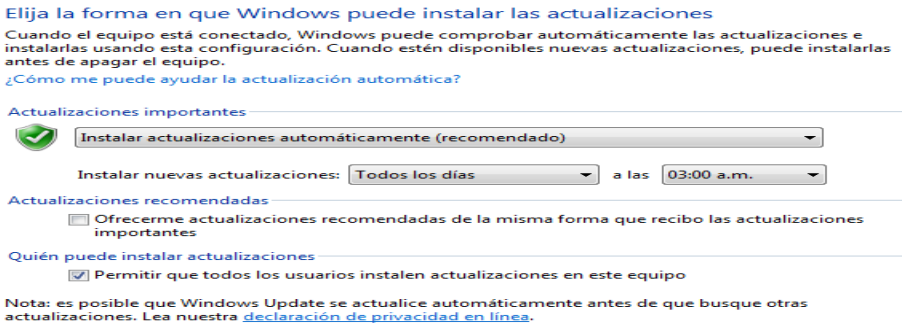
Activar el firewall



Fuente: Elaboración Propia.

Figura 25

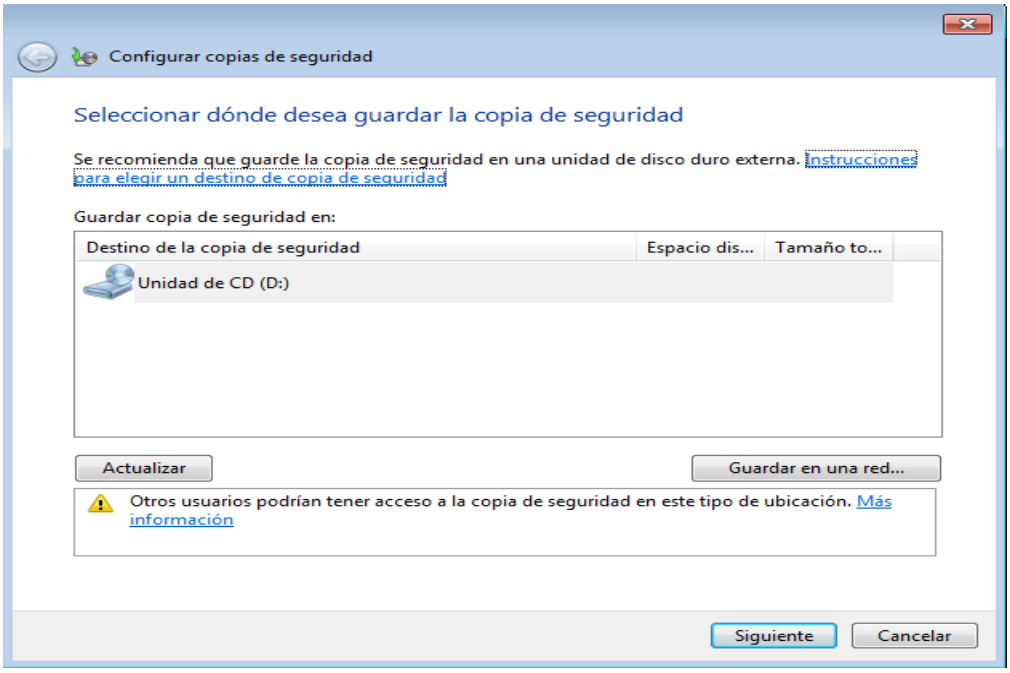
Activar la opción de actualización automática de Windows Update



Fuente: Elaboración Propia.

Figura 26

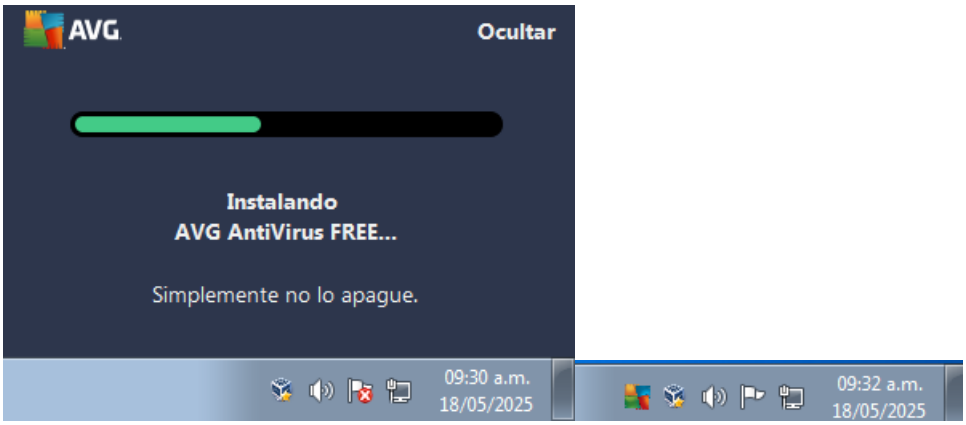
Generar una copia de seguridad



Fuente: Elaboración Propia.

Figura 27

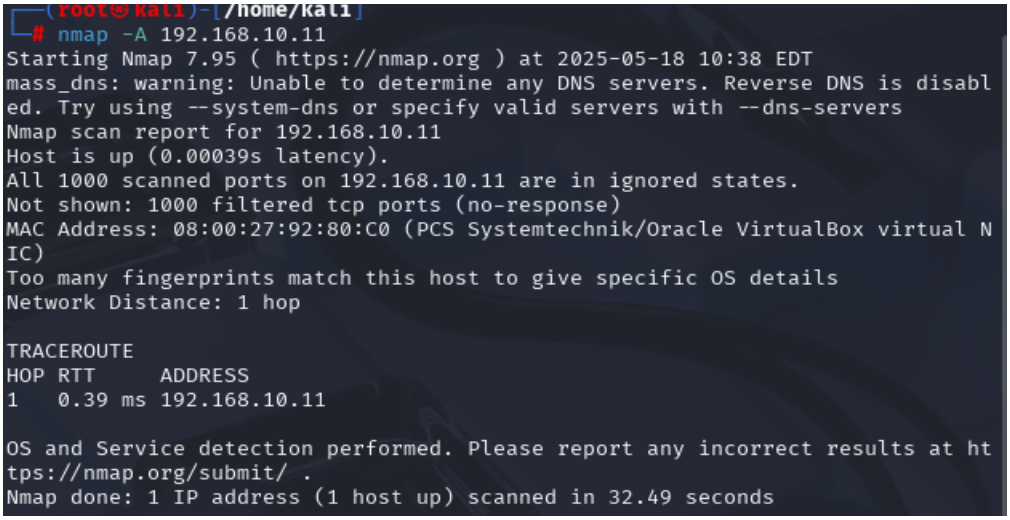
Instalar un antivirus



Fuente: Elaboración Propia.

Figura 28

Verificar nuevamente puertos y servicios



Fuente: Elaboración Propia.

Como se observa en la ilustración 13 nmap ya no puede verificar puertos y servicios, por ende, las correcciones realizadas a las alertas del centro de actividades funciono. Lo

recomendable seria cambiar el sistema operativo a uno mas actual con actualizaciones de Windows Defender y Windows Update, pero por las condiciones actuales de la organización se puede manejar el problema de esta manera.

Diferencias entre un equipo Blue Team y un equipo de Respuesta a Incidentes Informáticos (CSIRT)

Si bien ambos equipos están alineados a los objetivos de defensa y protección de la infraestructura tecnológica, existen diferencias claras en su enfoque, alcance y metodología.

El equipo Blue Team tiene como función principal prevenir, detectar y mitigar amenazas, desde una perspectiva continua y estructural. Se encarga del monitoreo de sistemas, implementación de políticas de seguridad, gestión de vulnerabilidades, endurecimiento (hardening) de sistemas y análisis de comportamientos anómalos. Su trabajo es constante y proactivo, enfocado en fortalecer la postura de ciberseguridad institucional antes de que ocurran incidentes.

Por otro lado, CSIRT actúa posterior o durante un evento de seguridad, con la finalidad de contener, investigar, erradicar y recuperar los activos afectados. Su función es reactiva y táctica, enfocada en la gestión del ciclo de vida de incidentes (detección, análisis, contención, erradicación, recuperación y retroalimentación). (Codespace Academy, 2022)

¿Para qué se utilizaría el marco del CIS (Center for Internet Security) en un equipo Blue Team?

Dentro del equipo Blue Team se me indicara utilizar las guías del CIS, su aplicación se centraría principalmente en establecer y validar configuraciones seguras para sistemas

operativos, servidores, dispositivos de red y aplicaciones, a través de los denominados CIS Benchmarks.

Estas guías proporcionan estándares técnicos detallados y consensuados, orientados al endurecimiento de sistemas, con el fin de reducir la superficie de ataque y mitigar vulnerabilidades conocidas. Además, se podrían emplear los CIS Critical Security Controls (v8) como marco de referencia para la implementación de controles técnicos y administrativos prioritarios, aplicando una estrategia defensiva basada en riesgos y madurez organizacional.

Por tanto, en un entorno Blue Team, el CIS se utiliza como una herramienta normativa y operativa para la definición de políticas de configuración segura, evaluación de cumplimiento y verificación de medidas preventivas y de monitoreo. (ManageEngine, 2024)

Funciones y características principales de un SIEM

Un SIEM (Security Information and Event Management) es una herramienta esencial en la defensa informática moderna, especialmente en entornos Blue Team. Su principal objetivo es centralizar, correlacionar y analizar registros (logs) de diversos sistemas, dispositivos y aplicaciones, para detectar patrones anómalos, eventos de seguridad y amenazas potenciales en tiempo real. (MarcadorDePosición1; Ámbit BST, 2022; MarcadorDePosición1)

Funciones principales:

Recolección de eventos y registros: Recibe logs desde firewalls, servidores, aplicaciones, bases de datos, controladores de dominio, entre otros.

Normalización y almacenamiento: Transforma los eventos heterogéneos en un formato común que facilita su análisis posterior.

Correlación de eventos: Establece reglas para detectar secuencias de actividades sospechosas, como varios intentos de inicio de sesión fallidos seguidos de acceso exitoso desde una IP anómala.

Generación de alertas: Notifica a los analistas de seguridad sobre posibles incidentes para permitir respuestas tempranas.

Análisis forense: Permite reconstruir eventos de seguridad pasados, útil en auditorías y respuesta a incidentes.

Cumplimiento normativo: Facilita la auditoría en estándares como ISO/IEC 27001, NIST, PCI-DSS, entre otros.

Características destacadas:

Escalabilidad y soporte para entornos híbridos (on-premise / nube).

Capacidad de integración con soluciones SOAR (Security Orchestration, Automation and Response).

Interfaces visuales para dashboards e informes personalizados.

Algunos SIEM conocidos bajo licencia libre o comunitaria incluyen Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana) y OSSIM de AlienVault. Que ayudarían a la organización en estos momentos.

Herramientas de contención de ataques informáticos

A diferencia de las herramientas de detección (IDS, SIEM, etc.), las herramientas de contención se centran en limitar, bloquear o mitigar el impacto de un ataque en tiempo real, evitando su propagación o persistencia. A continuación, se presentan tres ejemplos representativos:

Firewall de próxima generación (NGFW):

Estos dispositivos o aplicaciones actúan como barreras activas que inspeccionan el tráfico a nivel de aplicación, identificando y bloqueando tráfico malicioso. Integran funciones como control de aplicaciones, filtrado web, VPN, e incluso capacidades antimalware y de prevención de intrusos. (VMware, 2023)

Ejemplo: pfSense (software libre y robusto), FortiGate, Palo Alto NGFW.

EDR (Endpoint Detection and Response):

Las plataformas EDR no solo detectan comportamientos maliciosos en los endpoints, sino que permiten acciones de contención como el aislamiento del dispositivo, la terminación de procesos, y la eliminación de archivos maliciosos en tiempo real.

Ejemplo: Wazuh con OSSEC (GPL), CrowdStrike Falcon, SentinelOne.

Wazuh es una plataforma de seguridad de código abierto (open-source) que se utiliza para detección de intrusiones, monitoreo de integridad, análisis de logs, detección de malware, y respuesta ante incidentes. Su arquitectura está basada en un modelo cliente-servidor, donde los agentes Wazuh se instalan en los endpoints (servidores, estaciones de trabajo, contenedores, etc.),

y estos envían datos al servidor Wazuh, que luego los procesa y visualiza en una interfaz centralizada basada en Kibana (Elasticsearch). (Wazuh, 2024)

Funcionalidades clave:

HIDS (Host-based Intrusion Detection System): Permite detectar comportamientos sospechosos en los sistemas monitoreados.

Análisis de logs: Recoge, analiza y correlaciona eventos a partir de registros del sistema, aplicaciones y dispositivos.

Control de integridad (FIM): Supervisa archivos sensibles y alerta sobre cambios no autorizados.

Inventario del sistema: Recopila información sobre el software instalado, puertos abiertos, procesos en ejecución, etc.

Cumplimiento normativo: Facilita la alineación con estándares como PCI-DSS, HIPAA, GDPR y NIST mediante reglas y reportes preconfigurados.

Respuesta ante incidentes: Puede ejecutar acciones automáticas o manuales como parte de una estrategia de contención y mitigación.

Integraciones frecuentes:

Elasticsearch + Kibana: Wazuh suele desplegarse junto al stack ELK para visualizar y analizar eventos.

Firewalls, antivirus, sistemas de autenticación: Puede correlacionar datos de múltiples fuentes.

Usos comunes:

Monitoreo de seguridad en entornos empresariales, soporte en auditorías de cumplimiento, análisis forense posterior a incidentes.

Vigilancia de infraestructuras críticas (servidores, contenedores, cloud, etc.).

Control de acceso a red (NAC – Network Access Control):
Soluciones NAC restringen o segmentan el acceso a la red basado en políticas. Por ejemplo, pueden aislar automáticamente un equipo comprometido o no conforme, redireccionándolo a una zona de cuarentena. (Fortinet, 2023)

Ejemplo: PacketFence (open source), Cisco ISE.

Estas herramientas deben estar integradas dentro de un plan estratégico de respuesta y recuperación, priorizando la contención rápida para evitar daños colaterales y preservar la continuidad operativa.

Conclusiones

El desarrollo del laboratorio evidenció que el enfoque de ciberseguridad debe combinar habilidades técnicas ofensivas y defensivas, pero también una profunda comprensión legal y ética que permita actuar de manera responsable en entornos altamente sensibles.

El análisis de los contratos reveló cláusulas abusivas e inconstitucionales, que contravienen la Ley 1273 de 2009 y los principios éticos del COPNIA, y que podrían convertir al profesional en cómplice de delitos informáticos si no se identifican a tiempo.

La simulación del ataque a través de MS17-010 demostró cómo sistemas desactualizados con SMBv1 habilitado representan una puerta de entrada crítica, lo que refuerza la necesidad de mantener políticas estrictas de actualización y hardening de sistemas.

La fase de contención Blue Team reafirmó la importancia de procedimientos de respuesta estructurados, como el aislamiento de sistemas, recolección de evidencia forense y análisis de logs, que permiten enfrentar ataques sin comprometer la cadena de custodia ni la estabilidad del entorno operativo.

Recomendaciones

Implementar revisiones legales rigurosas de todos los contratos laborales y acuerdos de confidencialidad

Las organizaciones deben evitar aceptar cláusulas que vulneren derechos fundamentales o que prohíban denunciar conductas ilícitas. Es imperativo que los contratos sean revisados por equipos jurídicos especializados en derecho informático, asegurando cumplimiento con las leyes. La ética profesional debe prevalecer sobre intereses corporativos que pretendan encubrir malas prácticas.

Adoptar políticas estrictas de actualización de sistemas y eliminación de tecnologías obsoletas

El caso expuesto evidenció cómo el uso de sistemas operativos desactualizados (como Windows 7) con servicios inseguros habilitados (como SMBv1) facilita la explotación remota. Se recomienda establecer cronogramas de actualización tecnológica y aplicar configuraciones seguras alineadas con los CIS Benchmarks y boletines de seguridad oficiales como MS17-010.

Desarrollar capacidades internas de respuesta a incidentes con un enfoque estructurado

Las organizaciones deben conformar equipos Blue Team con entrenamiento específico en respuesta a incidentes (CSIRT), apoyados en marcos internacionales como el NIST SP 800-61r2. Deben estar preparados para actuar con celeridad, preservando evidencia digital y mitigando el daño, sin comprometer la integridad del sistema ni la cadena de custodia.

Fomentar la cultura ética, técnica y legal en el talento humano

Es crucial que el personal técnico comprenda el alcance de su responsabilidad profesional. Las

organizaciones deben promover programas de formación continua en normativas, reforzando el principio de no complicidad frente a actos contrarios al ordenamiento jurídico.

Integrar herramientas de análisis y monitoreo con licencias abiertas

Frente a limitaciones presupuestarias, existen soluciones robustas de código abierto como Wazuh, ELK Stack, TCPView o Wireshark. Estas herramientas permiten desarrollar capacidades avanzadas de monitoreo, detección y contención sin incurrir en altos costos, lo que democratiza el acceso a la seguridad informática sin sacrificar calidad ni cobertura.

Establecer mecanismos de auditoría y control sobre el uso de herramientas forenses

Es fundamental implementar sistemas de control de acceso, trazabilidad y auditoría sobre el uso de herramientas de análisis forense y administración de datos sensibles. Esto incluye autenticación multifactor, registros de actividad (logs), y políticas claras sobre los límites del análisis digital, todo ello en línea con los principios de minimización y finalidad definidos en la Ley 1581 de 2012.

Conformar comités éticos y técnicos para supervisar actividades críticas

Para prevenir el indebido manejo de herramientas y técnicas de intrusión, las organizaciones deben establecer comités interdisciplinarios que evalúen previamente cualquier acción de pentesting, análisis forense o simulación ofensiva, especialmente en entornos sensibles. Esto garantiza la transparencia y el cumplimiento de la normativa vigente.

Referencias

Ámbit BST. (15 de Marzo de 2022). *¿Qué significa SIEM y cómo funciona?* Obtenido de Ámbit BST: https://www.ambit-iberia.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

CIS. (8 de mayo de 2021). *CIS Controls v8*. Obtenido de Center for Internet Security: https://www.cisecurity.org/controls/v8

Codespace Academy. (27 de abril de 2022). *¿En qué se diferencia un equipo Blue Team de un CSIRT?* Obtenido de Codespace Academy: https://codespaceacademy.com/csirt-trabajo-blueteam/

Congreso de Colombia. (09 de octubre de 2003). *Ley 842 de 2003: Por la cual se reglamenta el ejercicio de la ingeniería y se expide el Código de Ética Profesional*. Obtenido de Consejo Profesional Nacional de Ingeniería – COPNIA: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Congreso de Colombia. (5 de enero de 2009). *Ley 1273 de 2009*. Obtenido de Departamento Administrativo de la Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (18 de octubre de 2012). *Ley 1581 de 2012*. Obtenido de Departamento Administrativo de la Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Consejo Profesional Nacional de Ingeniería – COPNIA. (2003). *Código de Ética Profesional de los Ingenieros*. Obtenido de copnia: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Fortinet. (2023). *What is Network Access Control (NAC)?* Obtenido de Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-network-access-control

Greenbone AG. (2023). *OpenVAS*. Obtenido de Greenbone: https://www.greenbone.net/en/openvas/

INCIBE. (2025). *Pentesting*. Obtenido de INCIBE - Aprende Ciberseguridad: https://www.incibe.es/aprendeciberseguridad/pentesting#:~:text=El%20Concepto,vulnerabilidades%20para%20prevenir%20ataques%20externos.

Kali Linux. (28 de mayo de 2025). *Enum4linux*. Obtenido de Kali Tools: https://www-kali-org.translate.goog/tools/enum4linux/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

KeepCoding. (2021). *Herramientas de postexplotación*. Obtenido de KeepCoding Blog: https://keepcoding.io/blog/herramientas-de-postexplotacion/

Maltego Technologies GmbH. (2023). *Maltego*. Obtenido de Maltego: https://www.maltego.com/

ManageEngine. (2024). *Controles de seguridad crítica CIS*. Obtenido de ManageEngine: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

NIST. (2012). Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST. (1 de agosto de 2012). *Computer Security Incident Handling Guide (SP 800-61 Revision 2)*. Obtenido de National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Nmap Project. (2023). *Manual de Nmap en español*. Obtenido de Nmap: https://nmap.org/man/es/index.html

Norma ISO 27001. (11 de julio de 2013). *Evaluación del desempeño en ISO 27001.* Obtenido de Norma ISO 27001: https://www.normaiso27001.es/evaluacion-del-desempeno-en-iso-27001/

OEA. (28 de mayo de 2025). *Sección de Ciberseguridad del CICTE*. Obtenido de Organización de los Estados Americanos: https://www.oas.org/ext/es/principal/oea/nuestra-estructura/sg/ssm/cicte/seccion-ciberseguridad

Offensive Security. (diciembre de 2023). *About Exploit Database*. Obtenido de Exploit Database: https://www.exploit-db.com/about-exploit-db

openvas.org. (2025). Obtenido de https://www.openvas.org/

Orebaugh, K. S. (2008). *NIST.* Obtenido de Technical Guide to Information Security Testing and Assessment (SP 800-115): https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Rapid7. (2023). *Metasploit Framework*. Obtenido de Metasploit: https://www.metasploit.com/

Tableau Software. (28 de mayo de 2024). *Página oficial de Tableau*. Obtenido de Tableau: https://www.tableau.com/

The MITRE Corporation. (17 de 03 de 2017). *CVE-2017-0144: Windows SMB remote code execution vulnerability*. Obtenido de CVE – Common Vulnerabilities and Exposures: https://www.cve.org/CVERecord?id=CVE-2017-0144

VMware. (2023). *What is a Next-Generation Firewall (NGFW)?* Obtenido de VMware: https://www.vmware.com/topics/next-generation-firewall

Wazuh. (2024). *Plataforma de detección y respuesta de código abierto*. Obtenido de Wazuh: https://wazuh.com/

Wazuh. (15 de abril de 2024). *Use cases*. Obtenido de Wazuh Documentation: https://documentation.wazuh.com/current/getting-started/use-cases/index.html