Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Damaris Nathaly Pabón Jaimes

Asesor

Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Basicas, Tecnología e ingeniería - ECBTI

Programa Especialización en Seguridad Informática

2025

Resumen

Este informe presenta un análisis integral de las capacidades técnicas, legales y éticas que deben poseer los equipos Red Team y Blue Team. En el ámbito de la ciberseguridad organizacional se exploran fundamentos normativos clave, metodologías de prueba de penetración, escenarios de simulación ofensiva y medidas de contención. El propósito es destacar la importancia de una estrategia coordinada entre ambos equipos para fortalecer la postura de seguridad digital, garantizar el cumplimiento legal y fomentar una cultura ética en entornos digitales.

***Palabras clave*:** Ciberseguridad, Red Team, Blue Team, Ética, Pentesting.

Abstract

This report presents a comprehensive analysis of the technical, legal, and ethical capabilities required by Red Team and Blue Team members. Within the field of organizational cybersecurity, it explores key regulatory frameworks, penetration testing methodologies, offensive simulation scenarios, and containment measures. The purpose is to highlight the importance of a coordinated strategy between both teams to strengthen the digital security posture, ensure legal compliance, and promote an ethical culture in digital environments.

***Keywords*:** Cybersecurity, Red Team, Blue Team, Ethics, Pentesting.

Glosario

Auditoría de seguridad: Proceso sistemático de evaluación de la infraestructura tecnológica de una organización, con el fin de identificar vulnerabilidades, verificar el cumplimiento de políticas de seguridad y proponer mejoras.

Blue Team: Equipo encargado de la defensa activa de los sistemas informáticos mediante la implementación de controles de seguridad, monitoreo y respuesta ante amenazas.

Ciberespionaje: Práctica ilegal para obtener información confidencial de manera encubierta a través de medios digitales, generalmente con fines políticos, económicos o estratégicos, sin el consentimiento del titular de la información.

CIS Benchmarks: Conjunto de guías desarrolladas por el Center for Internet Security con configuraciones seguras recomendadas para sistemas operativos, software y dispositivos.

Confidencialidad: Principio fundamental de la seguridad de la información que garantiza que los datos sensibles solo sean accesibles por personas autorizadas, protegiéndolos contra el acceso no autorizado o la divulgación indebida.

Contención: Acción orientada a limitar o detener el avance de una amenaza informática una vez ha sido detectada, evitando su propagación.

Escalada de privilegios: Técnica utilizada durante un ataque que permite a un usuario con permisos limitados obtener privilegios administrativos en un sistema comprometido.

Ética profesional: Conjunto de principios y valores que regulan la conducta de los profesionales en el ejercicio de su labor, promoviendo el respeto por la ley y la honestidad, la responsabilidad y el bien común.

Exploit: Fragmento de código, secuencia de comandos o software que aprovecha una vulnerabilidad en un sistema para ejecutar acciones no autorizadas como acceder, modificar o dañar información.

Hardenización: Proceso de fortalecimiento de la configuración de sistemas y redes para reducir vulnerabilidades y minimizar la superficie de ataque.

Legislación informática: Conjunto de normas legales que regulan el uso de las tecnologías de la información, estableciendo responsabilidades, derechos y sanciones relacionados con los delitos informáticos y la protección de datos personales.

Ley 1273 de 2009: Legislación colombiana que modifica el Código Penal para incluir delitos informáticos, protegiendo la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos.

Meterpreter: Herramienta avanzada de explotación incluida en Metasploit, que proporciona una consola para controlar remotamente un sistema comprometido, permitiendo ejecutar comandos y escalar privilegios.

Pentesting (Pruebas de penetración): Proceso sistemático mediante el cual se simulan ataques a sistemas informáticos con el objetivo de identificar vulnerabilidades que puedan ser explotadas por actores maliciosos.

PoC (Proof of Concept): Prueba de concepto técnica que demuestra la viabilidad de una vulnerabilidad explotada.

Red Team: Conjunto de profesionales de seguridad informática que se encargan de simular ataques ofensivos controlados para poner a prueba la eficacia de las defensas de una organización.

SIEM (Security Information and Event Management): Solución que centraliza, analiza y correlaciona eventos de seguridad generados por distintos dispositivos para detectar amenazas y apoyar la respuesta a incidentes.

Vulnerabilidad: Debilidad o falla en un sistema informático que puede ser explotada por atacantes, comprometiendo la seguridad o su funcionamiento.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Introducción

El nivel de sofisticación actual de los ataques informáticos ha llevado a las organizaciones a adoptar estrategias duales que integren ofensiva (Red Team) y defensiva (Blue Team). Este informe documenta el proceso formativo, técnico y ético que permite desarrollar competencias esenciales en estos roles, fortaleciendo la protección de activos digitales, el cumplimiento normativo y la actuación ética en el ámbito de la seguridad informática.

Objetivos

Objetivo General

Fortalecer las capacidades técnicas, legales y éticas para el diseño e implementación de estrategias de ciberseguridad mediante la integración de roles Red Team y Blue Team en entornos organizacionales.

Objetivos Específicos

- Identificar los fundamentos legales que rigen la actuación de los equipos de seguridad informática en Colombia.
- Aplicar metodologías de pruebas de penetración para simular ataques controlados.
- Desarrollar capacidades de contención y mitigación desde el enfoque de Blue Team.
- Evaluar implicaciones éticas en la toma de decisiones en escenarios reales de ciberseguridad.

Desarrollo del Informe

Fundamentos legales y técnicos en ciberseguridad: Red Team & Blue Team.

Durante la primera fase de verificación en ciberseguridad se abordaron los aspectos fundamentales que rigen las prácticas de seguridad ofensiva y defensiva en entornos organizacionales. Este conocimiento es esencial para que los equipos Red Team & Blue Team operen bajo criterios técnicos sólidos y marcos normativos establecidos, con el fin de reducir riesgos y garantizar la integridad de los activos digitales.

Marco Legal Aplicado a la Ciberseguridad.

La actuación tanto del Red Team como del Blue Team debe estar enmarcada en la legislación vigente en Colombia, dos leyes fundamentales regulan la ciberseguridad:

La Ley 1273 de 2009 tipifica delitos como el acceso abusivo a sistemas, el uso de software malicioso y la interceptación de datos sin autorización, entre otros (Congreso de Colombia, 2009). Esta ley protege los activos informáticos como un bien jurídico y sanciona los ataques contra la confidencialidad, integridad y disponibilidad de la información.

La Ley 1581 de 2012, por su parte, establece los principios y obligaciones para el tratamiento adecuado de datos personales, reconociendo derechos a los titulares y facultades de inspección a la Superintendencia de Industria y Comercio (Congreso de Colombia, 2012).

Ambas leyes son esenciales para guiar las actividades de evaluación de seguridad. Pues aseguran que las acciones técnicas no vulneren los derechos de los usuarios ni excedan los límites éticos.

Acciones del Red Team, Simulación de Ataques Éticos.

El equipo Red Team tiene como objetivo identificar vulnerabilidades simulando ataques reales de manera controlada. Para lograrlo se siguió una metodología de Pentesting compuesta por 6 fases esenciales:

Reconocimiento:

Durante esta etapa se recopila información sobre el objetivo que puede ser una red, un servidor, un sitio web o cualquier sistema informático sin interactuar directamente con él, se investiga todo lo posible desde fuentes públicas.

Escaneo:

Para la etapa de escaneo se realiza una exploración más directa del objetivo con el fin de identificar puertos abiertos, servicios activos y posibles vulnerables.

Enumeración y análisis de vulnerabilidades:

Durante esta fase se recolecta información aún más detallada sobre los servicios detectados y se identifican posibles vulnerabilidades específicas.

Explotación:

Se intentan explorar las diferentes vulnerabilidades encontradas para acceder al sistema. Esta es la etapa más delicada del proceso, pues se simula un ataque real.

Escalada de Privilegios:

Una vez se tiene acceso al sistema, el siguiente paso es aumentar los privilegios para obtener más control de los recursos y ver hasta qué punto se puede comprometer el sistema.

Análisis y Reporte:

Finalmente, se documentan todos los hallazgos de vulnerabilidades que se encontraron, cómo se explotaron y qué riesgos representan, también se incluyen recomendaciones para mitigar los problemas.

Este enfoque permite evaluar objetivamente la exposición de la infraestructura tecnológica y construir una base para fortalecer la seguridad interna (Zuluaga, 2017).

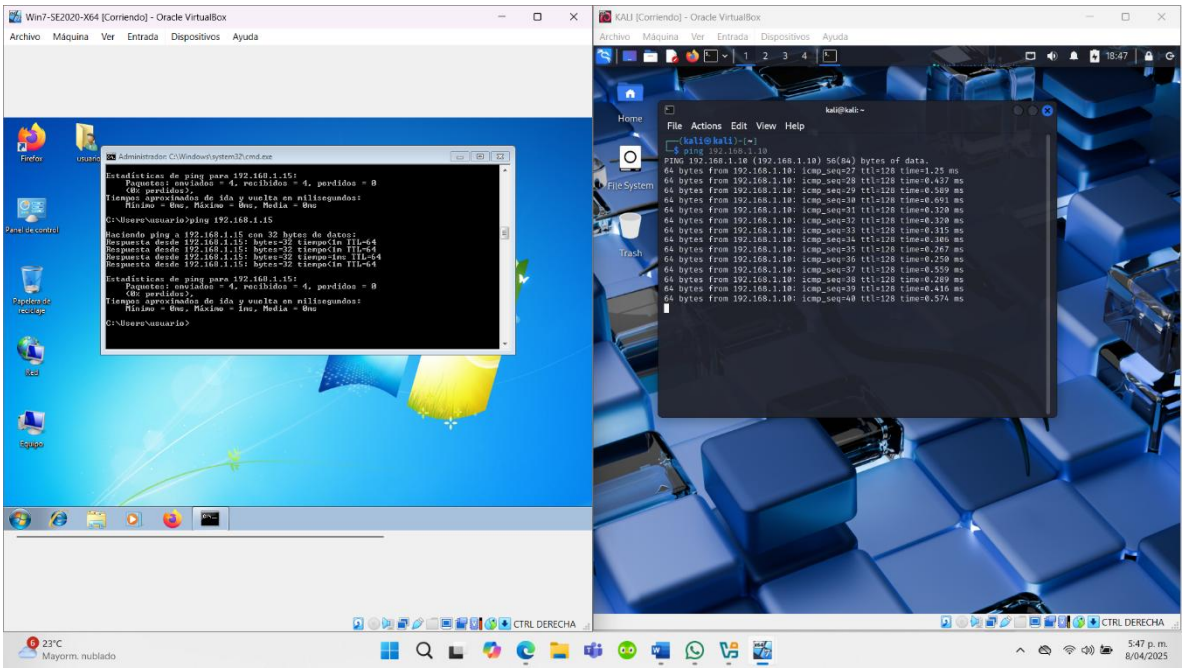
Acciones del Blue Team, Detección y Contención

El equipo Blue Team opera en paralelo para detectar, responder y mitigar incidentes de seguridad. En esta etapa se configuró un laboratorio virtual compuesto por 2 máquinas con Windows 7 y Kali Linux. Estas se ejecutaron en VirtualBox y se conectaron en red para simular un entorno real.

A través de este entorno se aplicaron prácticas de monitoreo y validación de conectividad. Las 2 máquinas virtuales comparten características similares en términos de recursos de hardware:

- Memoria RAM: 2048 MB (2GB) para cada máquina.
- Procesadores asignados:
    - Kali: 2 procesadores virtuales.
    - Windows 7: 1 procesador virtual.
- Almacenamiento:
    - Windows 7: 50GB.
    - Kali: 80GB

Figura 1
Ejecución de ping entre máquinas virtuales.



Nota. Autoría Propia.

El laboratorio sirvió como campo de entrenamiento para consolidar las competencias técnicas en ambientes controlados (Quintero, 2020).

Integración Legal-Técnica en Escenarios Prácticos.

La interacción entre los enfoques ofensivo y defensivo debe estar mediada por un marco ético y legal. El conocimiento técnico, sin comprensión normativa, puede derivar en actuaciones inapropiadas. Así, esta fase permitió comprender que la sinergia entre el Red Team y Blue Team no solo da en el ámbito técnico, sino en el cumplimiento de normativas, la trazabilidad de los procedimientos y la protección de los derechos digitales.

Como lo señalan Chindrus y Caruntu (2023), La colaboración entre ambos equipos dentro de entornos controlados mejora la capacidad de respuesta ante amenazas reales y fortalece la postura de ciberseguridad de la organización.

Actuación Ética Y Legal En Entornos De Ciberseguridad

En esta segunda etapa se verificaron casos que evidencian como el ejercicio de la ciberseguridad puede entrar en conflicto con principios éticos y normas legales cuando no se aplican controles, límites contractuales ni criterios de integridad profesional. Los escenarios propuestos por la organización CyberFort Technologies revelan la necesidad de consolidar una cultura de legalidad y transparencia, tanto en acuerdos contractuales como en el manejo de información sensible.

Irregularidades contractuales y principios vulnerados.

El análisis del acuerdo de confidencialidad presentado expone disposiciones que resultan contrarias a la normativa colombiana. La cláusula que prohíbe denunciar actividades ilegales viola el principio de legalidad, mientras que otras cláusulas trasladan la responsabilidad penal al trabajador, lo cual es jurídicamente inaceptable (Congreso de Colombia, 2009).

Desde una perspectiva ética, aceptar tales condiciones implicaría ignorar el deber profesional de actuar con lealtad hacia la sociedad y denunciar prácticas ilegales, tal como lo establece el Código de Ética de COPNIA (Copnia, 2015).

Delitos informáticos identificados.

Las condiciones del acuerdo y las prácticas internas de la empresa podrían configurar delitos según la Ley 1273 de 2009, como:

- Acceso abusivo a sistemas informáticos (Art. 269A)
- Violación de datos personales (Art. 269E)
- Uso de software malicioso (Art. 269F)

La aceptación pasiva de estas conductas convierte al profesional en cómplice por omisión, lo que compromete su responsabilidad legal (Congreso de Colombia, 2009).

Evaluación ética de una posible vinculación laboral.

Desde la perspectiva del profesional en ciberseguridad, aceptar un empleo en condiciones que encubren prácticas ilegales y trasladan culpas al trabajador representa una violación grave a la ética profesional y a los principios rectores de la ingeniería. El artículo 6 del Código de ética de Comunidad sigue denunciar actos contrarios a la ley y el artículo 10 prohíbe colaborar con personas que cometen dichos actos (Copnia, 2015).

Análisis del caso de Ciberespionaje.

El segundo escenario describe un acto de ciberespionaje durante una auditoría de seguridad realizada a un gobierno. Este acto, ejecutado por empleados de CyberFort Technologies, implicó la apropiación y comercialización de información sensible. Este tipo de conducta, además de vulnerar principios fundamentales como la confidencialidad y la responsabilidad, constituye una violación directa de la Ley 1273 y compromete la seguridad estatal (OAS, 2018).

Según Chindrus y Caruntu (2023), La confianza otorgada al personal de seguridad en ámbitos gubernamentales requiere mecanismos de control que prevengan el uso indebido del acceso privilegiado.

Límites éticos en el acceso a información crítica.

El acceso a información sensible por parte de una empresa de seguridad debe estar estrictamente regulado por contratos, limitando el alcance del servicio y controlado mediante trazabilidad, auditorías cruzadas y sistemas de monitoreo (MINTIC, 2022). El principio del mínimo privilegio y la responsabilidad compartida entre cliente y proveedor deben prevalecer para evitar abusos.

Mecanismos de supervisión y control recomendados.

Para prevenir el uso indebido de herramientas forenses se proponen 3 niveles de control:

- Técnico: Registro de logs, privilegios limitados, autenticación segura.
- Organizacional: Políticas de uso aceptable, validación doble y monitoreo de sesiones.
- De cumplimiento: Auditorías internas, comités de ética, canales protegidos de denuncia (Zuluaga, 2017).

Estos mecanismos garantizan la transparencia del proceso, protegen los derechos del cliente y previenen el abuso del poder técnico por parte del auditor.

Respuesta institucional frente al ciberespionaje.

Ante incidentes como el descrito, los gobiernos deben:

- Revocar contratos e iniciar acciones legales.
- Transparentar lo ocurrido y ajustar sus protocolos.
- Implementar sanciones ejemplares a las empresas infractoras.

Restaurar la confianza solo es posible mediante la redención de cuentas, la regulación efectiva y la formación ética continua en ciberseguridad (Quintero, 2020).

Simulación ofensiva y explotación controlada - Rol del Red Team.

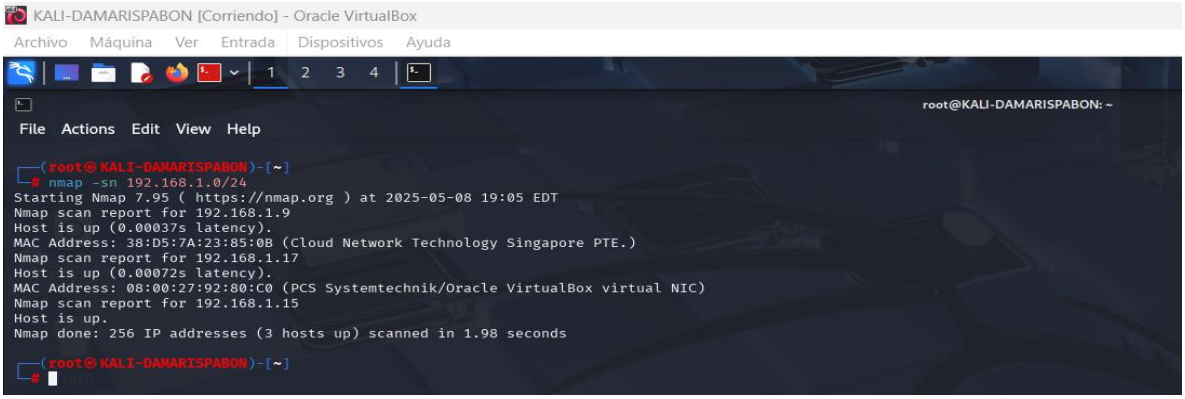
La tercera etapa del proceso formativo se centró en la ejecución práctica de una prueba de penetración controlada. El ejercicio desarrollado bajo los lineamientos del equipo Red Team, tuvo como propósito evidenciar como una vulnerabilidad real en una aplicación web puede ser identificada, explotada y utilizada para obtener acceso no autorizado a un sistema. La la simulación se realizó sobre una máquina con Windows con el servicio Rejetto HFS 2.3, permitiendo replicar un escenario realista de ataque.

Reconocimiento, escaneo y enumeración de servicios.

El proceso inició con tareas de reconocimiento activo y pasivo, utilizando herramientas como en Nmap y nbtscan para ampliar la red, identificar hosts activos y recolectar información preliminar sobre puertos abiertos y servicios disponibles. Estas herramientas son esenciales para cualquier operación ofensiva, pues permiten construir el mapa de superficie de ataque sin interactuar de forma destructiva con el objetivo (PandaSecurity, 2018).

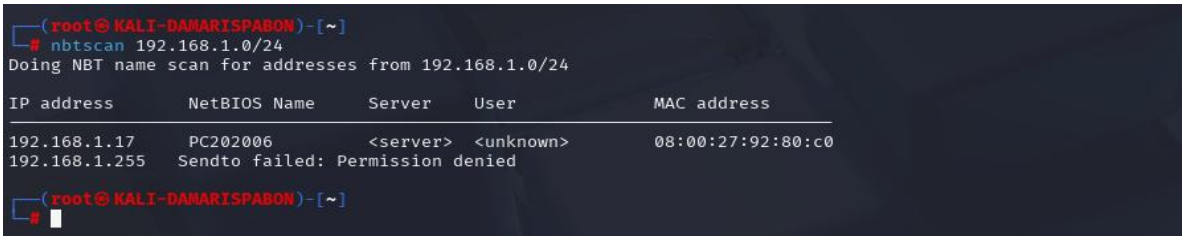
La etapa de escaneo incluyó la enumeración de servicios y la identificación de versiones específicas con el objetivo de detectar posibles vulnerabilidades explotables. Se identificó que el puerto 80 estaba en uso por el servicio vulnerable Rejetto HFS, Lo que orientó las siguientes fases de ataque.

Figura 2.
Resultados del Comando nmap -sn 192 168.1.0/24 para detección de host activos en la red local.



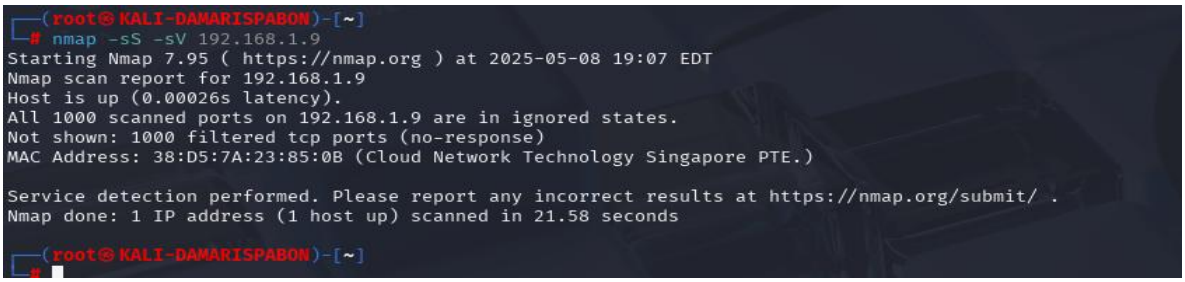
Nota. Autoría Propia.

Figura 3.
Verificación de nombres NetBIOS en la red de con el Comando nbtscan 192.168.1.0/24.



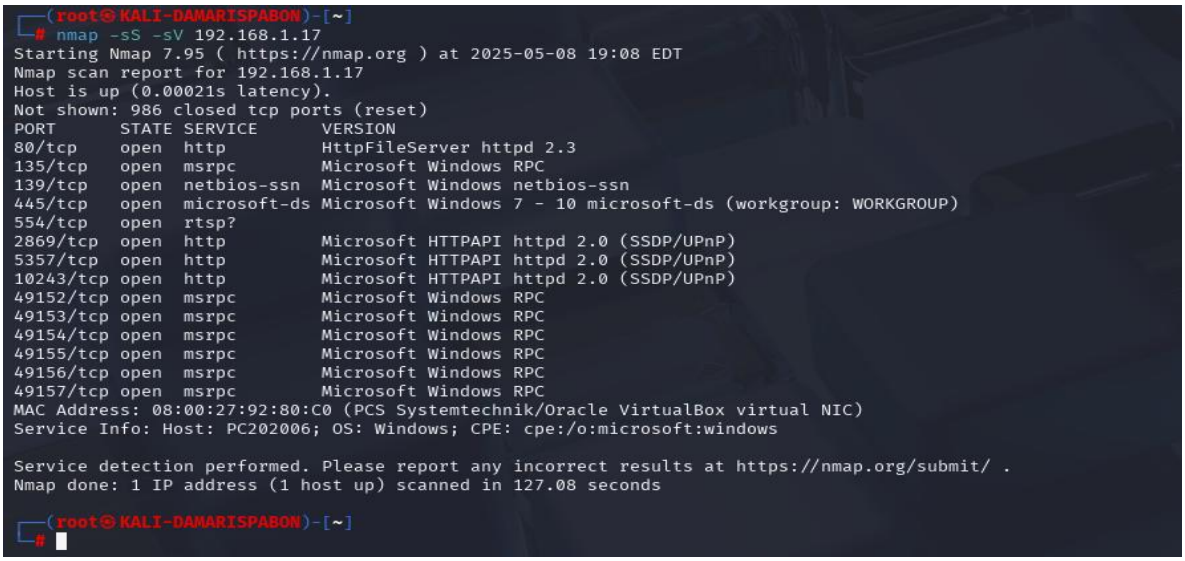
Nota. Autoría Propia.

Figura 4.
Escaneo de puertos con el Comando nmap -sS -sV 192.168.1.9 sin resultados.



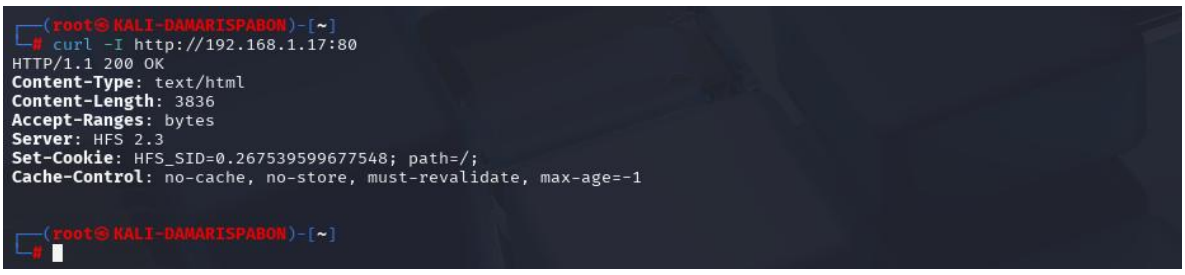
Nota. Autoría Propia.

Figura 5.
Escaneo de puertos con el Comando nmap -sS -sV 192.168.1.17 permitiendo identificar servicios y versiones en el host.



Nota. Autoría Propia.

Figura 6.
Verificación y análisis del contenido del servidor HFS con el comando curl -I http://192.168.1.17:80.



Nota. Autoría Propia.

Figura 7.
Exploración con NMAP usando el script nmap -f -script vuln 192.168.1.17 para identificar si la máquina virtual es vulnerable.

Nota. Autoría Propia.

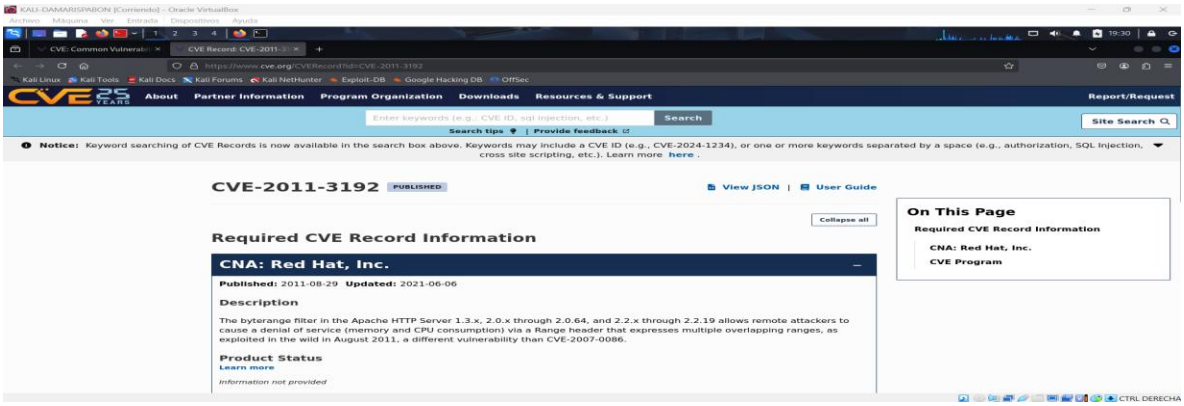
Análisis de vulnerabilidades y preparación de la explotación.

Una vez detectado el software vulnerable, se consultaron bases de datos como CVE.org, Exploit-DB y se utilizó la herramienta searchsploit para verificar la existencia de exploits

públicos. Se identificó que la versión de HFS contenía vulnerabilidades críticas, incluyendo la CVE-2014-6287, la cual permite ejecución remota de comandos (Revista Seguridad, 2018).

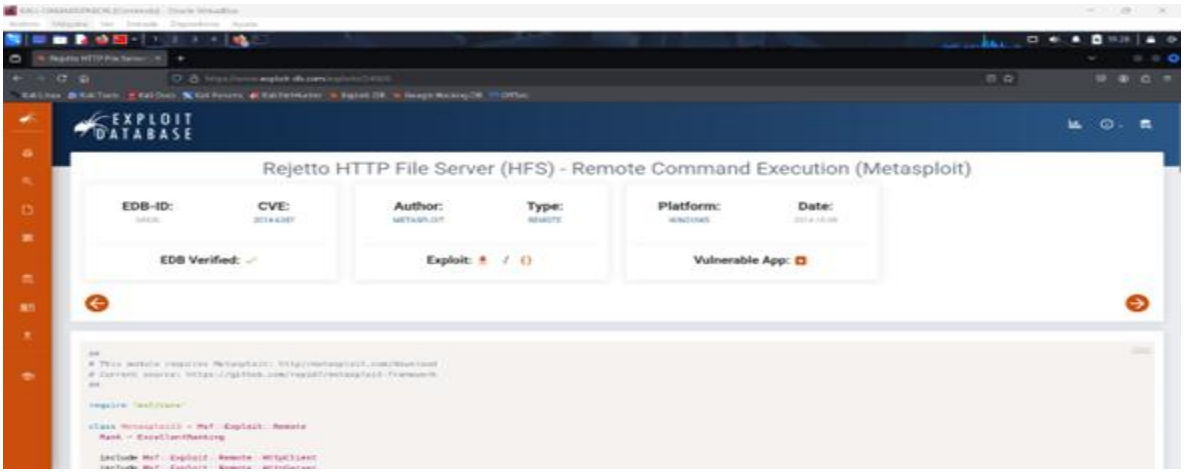
Con esta información se preparó el entorno para la explotación utilizando Metasploit Framework, cargando y configurando el exploit correspondiente a la vulnerabilidad identificada. La explotación exitosa permitió el acceso remoto a través de una sesión Meterpreter, controlando el sistema comprometido en tiempo real (Rapid7, 2012).

Figura 8.
Consulta de información técnica sobre la vulnerabilidad CVE-2011-3192 en el sitio oficial CVE(cve.org), como parte de la investigación previa al uso de exploits.



Nota. Autoría Propia.

Figura 9.
Consulta de información técnica en la página Exploit-DB sobre el exploit remoto para Rejetto HFS, vinculado a la CVE-2014-6287, útil para ejecución remota de comandos.



Nota. Autoría Propia.

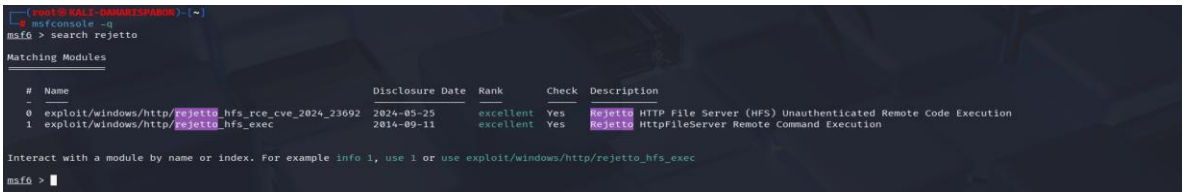
Figura 10.

Uso del comando searchsploit para buscar exploits disponibles para Rejetto HTTP File Server (HFS) en la base de datos local.

Nota. Autoría Propia.

Figura 11.

Se realiza la búsqueda de exploit relacionados con Rejetto en Metasploit.



Nota. Autoría Propia.

Figura 12.

Configuración del exploit HFS para intentar ejecución remota de código.

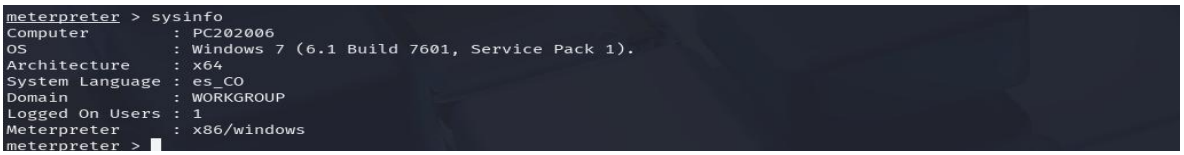
Nota. Autoría Propia.

Figura 13.

Ejecución del exploit con éxito, se abre una sesión meterpreter.

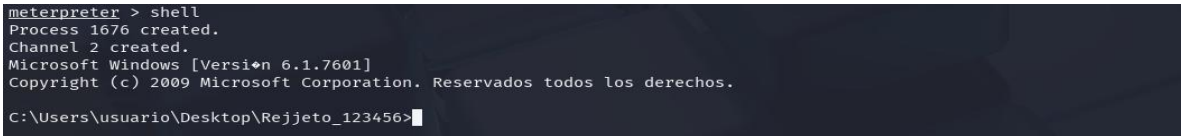
Nota. Autoría Propia.

Figura 14.
Se consulta la información del sistema comprometido desde meterpreter.



Nota. Autoría Propia.

Figura 15.
Se logra acceso directo a la línea de comandos del sistema víctima desde meterpreter.



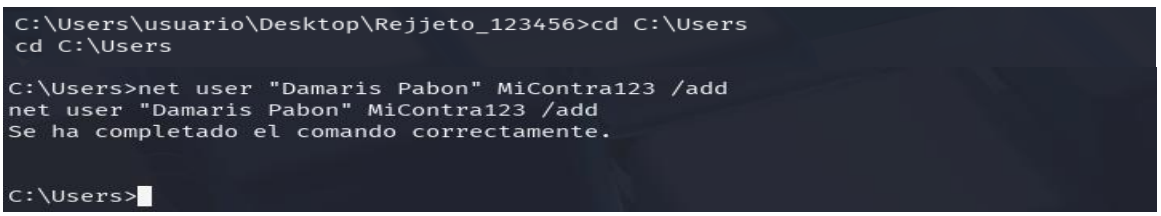
Nota. Autoría Propia.

Post-explotación: escalada de privilegios y persistencia.

Tras el acceso inicial, se ejecutaron tareas de post-explotación, enfocadas en escalar privilegios y establecer persistencia. Se creó un usuario local con privilegios administrativos y se utilizaron técnicas de token impersonation mediante el módulo incognito de Meterpreter, demostrando la viabilidad de un ataque prolongado en el sistema (Kotwani et al., 2023).

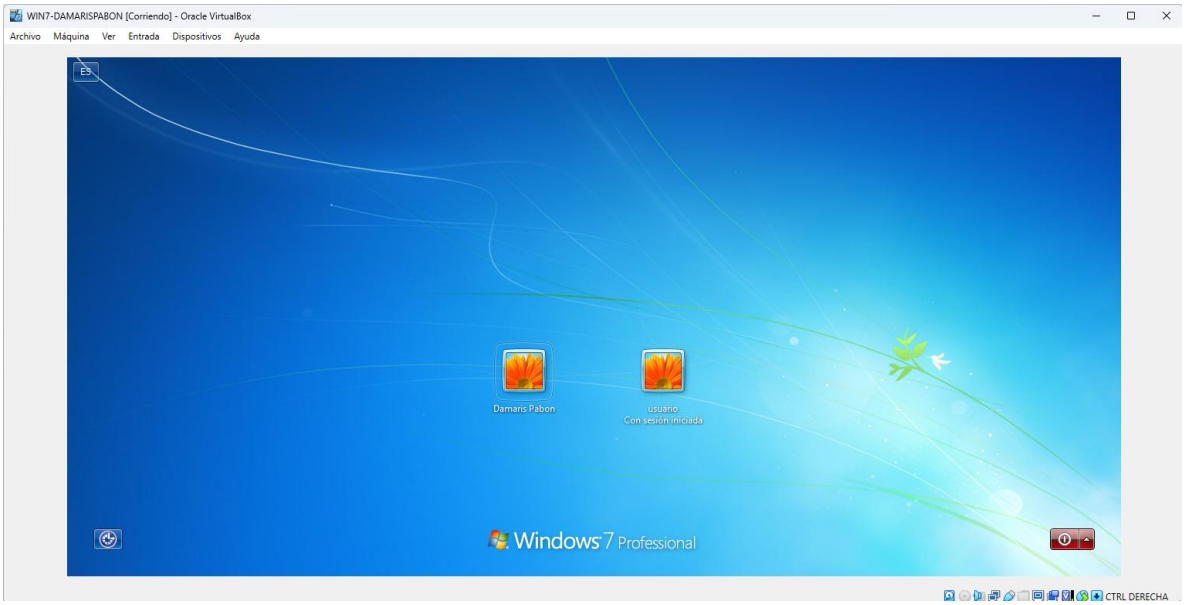
Estas acciones reflejan el riesgo real que representa un software no actualizado y mal configurado. La post-explotación no solo demuestra el acceso, sino que permite evaluar el impacto total de la brecha de seguridad. Incluyendo la capacidad de suplantar identidades y obtener el control total del sistema objetivo.

Figura 16.
Ejecución del comando net user "Damaris Pabon" MiContra123 /add para crear un nuevo usuario local con el nombre Damaris Pabon. El sistema confirma la correcta creación del usuario.



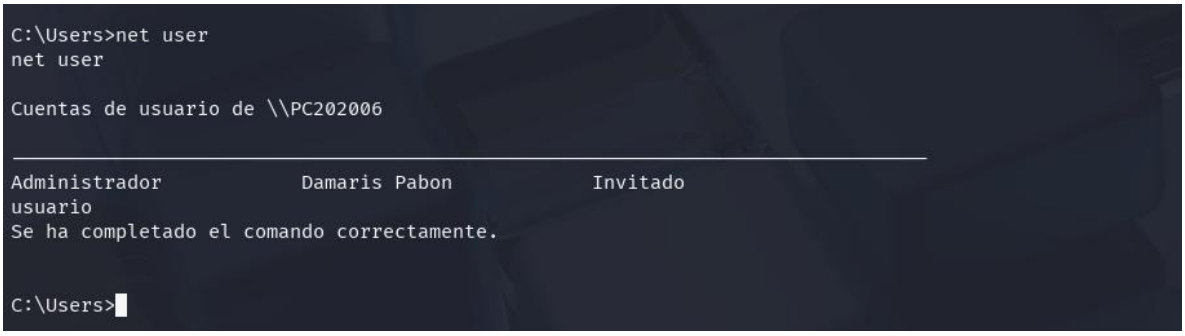
Nota. Autoría Propia.

Figura 17.
Inicio de sesión del sistema operativo Windows 7. Se puede visualizar la cuenta recién creada Damaris Pabon.



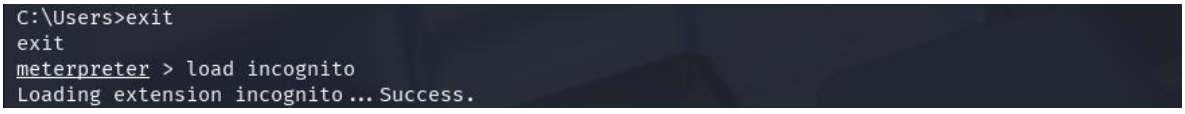
Nota. Autoría Propia.

Figura 18.
Ejecución del comando para listar todas las cuentas de usuario existentes en el sistema.



Nota. Autoría Propia.

Figura 19.
Se accede al entorno meterpreter y se carga la extensión incógnito usando el comando load incognito que permite manipular tokens para suplantar usuarios durante un ataque post explotación.



Nota. Autoría Propia.

Figura 20.
Se agrega al usuario Damaris Pabon al grupo de administradores del sistema mediante el comando add_localgroup_user "Administradores" "Damaris Pabon"desde meterpreter.

```
meterpreter > add_localgroup_user "Administradores" "DAmaris Pabon"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user DAmaris Pabon to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
```

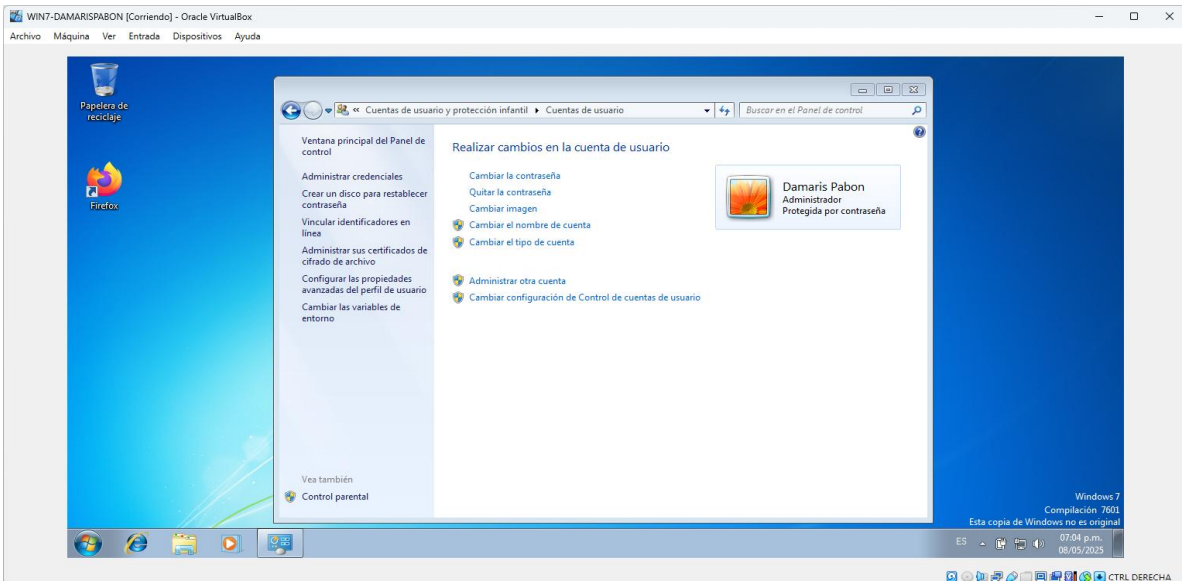
Nota. Autoría Propia.

Figura 21.
Ejecución del comando list_tokens -u dentro de meterpreter para listar los tokens de delegación e impersonación disponibles. Se identifican los tokens del sistema del usuario Damaris Pabon y usuario, útiles para realizar ataques de suplantación de identidad en el entorno comprometido.

```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\SYSTEM
PC202006\Damaris Pabon
PC202006\usuario

Impersonation Tokens Available
========================================
No tokens available

meterpreter >
```

Nota. Autoría Propia.

Figura 22.
Verificación de privilegios administrativos desde GUI.



Nota. Autoría Propia.

Reflexión estratégica.

Esta práctica permitió comprobar como una estrategia ofensiva bien ejecutada puede comprometer sistemas críticos si no se aplican políticas adecuadas de actualización y monitoreo. Al mismo tiempo, evidenció la importancia del Red Teaming como herramienta para fortalecer los controles de seguridad antes de que sean aprovechados por actores maliciosos (INCIBE, 2019).

Simulaciones como éstas refuerzan el enfoque proactivo en ciberseguridad y ayudan a las organizaciones a adoptar una postura más resiliente, permitiendo corregir vulnerabilidades antes de que se materialicen como incidentes reales.

Contención de ataques informáticos desde el enfoque del Blue Team.

En esta etapa se simula la respuesta inmediata ante un incidente de seguridad en tiempo real, priorizando acciones técnicas orientadas a la contención y mitigación del impacto. El ejercicio, enmarcado en un entorno sin herramientas comerciales. Destaca el papel del equipo Blue Team frente a incidentes, el uso de estándares abiertos como CIS Benchmarks y el valor de soluciones como SIEMs y firewalls libres para garantizar una respuesta efectiva en situaciones de compromiso.

Respuesta inmediata ante un ataque en curso.

Cuando se detecta un ataque en tiempo real, las acciones prioritarias del Blue Team incluyen:

- Aislar el sistema afectado de la red para evitar propagación y preservar evidencias (CCN Cert, 2018).

- Identificar el tipo de ataque, revisando procesos, registros y comportamiento anómalo mediante herramientas como Process Explorer o el visor de eventos de Windows (Zambrano Hernández et al., 2024).
- Preservar evidencia forense, incluyendo logs, capturas de pantalla y configuraciones actuales.
- Notificar al CSIRT o responsable de seguridad con documentación clara y precisa del incidente.
- Analizar posibles puntos de persistencia como cuentas de usuario creadas, servicios modificados o cambios en el registro del sistema (Rajendran et al., 2011).

Estas acciones deben documentarse y ejecutarse siguiendo un procedimiento normalizado, reforzando la trazabilidad.

Medidas de hardenización tras el ataque.

Tras contener el incidente, se deben aplicar prácticas de hardenización que esfuercen la postura de seguridad del sistema afectado. Las recomendaciones se alinean con los CIS benchmarks (CIS Security, 2020), e incluyen:

- Desactivar servicios innecesarios, como SMBv1 o remote Registry, que amplían la superficie de ataque (CCN Cert, 2018).
- Aplicar el principio de privilegio mínimo, evitando el uso extendido de cuentas administrativas.
- Establecer políticas de contraseñas robustas y activar autenticación multifactor.
- Auditar configuraciones clave del sistema operativo e implementar reglas de firewall específicas.

- Mantener el sistema actualizado cerrando brechas aprovechables por exploits conocidos.

Estas acciones bien documentadas reducen significativamente el riesgo de reinfección o escala futura (Zambrano Hernández et al., 2024).

Diferencias clave entre Blue Team y CSIRT

Aunque ambos equipos contribuyen a la ciberdefensa, su rol operativo varía.

Tabla 1.
Diferencias entre Blue Team y CSIRT

Rol	**Blue Team**	**Equipo de Respuesta a Incidentes (CSIRT)**
Enfoque	Proactivo – Prevención y monitoreo	Reactivo – Contención y análisis post-incidente
Funciones	Endurecimiento, monitoreo, detección	Contención, recuperación, análisis forense
Herramientas	SIEM, firewalls, benchmarks, antivirus	Forense, extracción de evidencia, recuperación
Ciclo de acción	Continuo y preventivo	Por evento, con retroalimentación a Blue Team

Nota. Autoría Propia.

Ambos equipos deben trabajar de forma coordinada, compartiendo hallazgos y mejorando continuamente la postura defensiva (Rajendran et al., 2011; Zambrano Hernández et al., 2024).

Acción práctica CIS benchmarks

Los CIS Benchmarks proporcionan guías detalladas para el hardening de sistemas operativos y aplicaciones. Como parte del Blue Team, su uso permite:

- Aplicar configuraciones seguras en sistemas Windows/Linux.
- Establecer controles prioritarios como el monitoreo de logs, inventario de activos y control de privilegios.
- Servir como referente de cumplimiento normativo e incluso en auditorías externas (CIS Security, 2020).
- Facilitar la implementación de seguridad en entornos sin presupuesto, ya que sus guías son de libre acceso.

Estas guías ayudan a establecer una base sólida de seguridad, especialmente en escenarios con recursos técnicos limitados.

Rol del SIEM en la contención y monitoreo.

Un SIEM (Security Information and Event Management) es esencial para:

- Centralizar y almacenar eventos desde múltiples fuentes.
- Correlacionar patrones sospechosos en tiempo real.
- Generar alertas e informes que apoyen al equipo de respuesta.
- Contribuir con el cumplimiento normativo y auditorías.

En entornos sin licencia comercial, soluciones como Wazuh o OSSIM permiten implementar estas funciones sin costo (Moreno, 2015). El SIEM complementa las tareas del Blue Team al ofrecer visibilidad integral del entorno.

Herramientas de contención sin costo.

pfSense (Firewall de red – Hardware/Software libre)

pfSense es una solución de firewall y router de código abierto que puede implementarse en dispositivos físicos o virtuales. Funciona como una barrera de contención perimetral al filtrar el tráfico entrante y saliente de una red con reglas definidas por el administrador.

Funciones de contención:

- Bloqueo inmediato de direcciones IP de origen malicioso.
- Segmentación de redes mediante VLANs o reglas por interfaz.
- Implementación de listas negras de acceso.
- Contención del tráfico durante una brecha o ataque DoS/DDoS.

Según el CIS Benchmarks, el uso de firewalls correctamente configurados es parte esencial de los controles fundamentales para limitar el movimiento lateral de amenazas dentro de una red (CIS Security, 2020).

Windows Defender Firewall (Software incluido en el sistema operativo).

El firewall nativo de Windows es una herramienta poderosa que, bien configurada, permite contener amenazas a nivel del host individual. Su ventaja principal es que ya viene integrado en sistemas Windows, por lo que no genera costo adicional y puede utilizarse inmediatamente en situaciones de emergencia.

Funciones de contención:

- Bloquear puertos específicos utilizados por malware o atacantes.
- Denegar conexiones entrantes/salientes por aplicación.
- Restringir el acceso a redes internas o externas durante una infección activa.

Zambrano Hernández et al. (2024) señala que el uso de firewalls locales es una técnica recomendada para confinar procesos sospechosos en el equipo infectado, limitando su capacidad de comunicación.

IPBlocker / Hosts File / Null Routing (Contención manual a nivel de sistema).

Estas son técnicas de contención local en las que se bloquea o redirige el tráfico a direcciones específicas consideradas maliciosas, ya sea mediante:

- Modificación del archivo hosts en sistemas operativos para impedir la resolución DNS hacia dominios utilizados por malware.
- Uso de comandos, como route add o iptables para crear rutas nulas a direcciones IP maliciosas.
- Implementación de scripts en PowerShell o Bash que bloquean tráfico a través de comandos de red.

Estas herramientas son eficaces para responder rápidamente a incidentes sin necesidad de instalar software adicional. Aunque rudimentarias, son especialmente útiles en entornos con restricciones presupuestarias, como lo indica el escenario del Anexo 5 (Zambrano Hernández et al., 2024).

- IPBlocker/Hosts file/Null Routing: Técnicas manuales para bloquear dominios o IPS maliciosas directamente desde el sistema sin depender de herramientas de terceros (Zambrano Hernandez et al., 2024).

Conclusiones

La implementación conjunta de estrategias ofensivas y defensivas evidencia que la sinergia entre Red Team y Blue Team fortalece significativamente la postura de seguridad informática de una organización, mientras el Red Team permite identificar vulnerabilidades reales mediante simulaciones controladas. El Blue Team desarrolla respuestas efectivas y resilientes ante amenazas, garantizando así una protección más robusta y proactiva de los activos digitales.

El cumplimiento de las leyes colombianas, como la Ley 1273 de 2009 y la Ley 1581 de 2012, así como la aplicación de principios éticos profesionales, es esencial para que los equipos de seguridad informática actúen dentro de límites aceptables. La legalidad y la ética deben ser los pilares que guíen cada acción, especialmente cuando se maneja información sensible o se simulan ataques que podrían tener consecuencias si no se realizan de forma adecuada.

Las simulaciones realizadas en entornos virtuales permitieron consolidar habilidades prácticas como la identificación de vulnerabilidades, explotación de sistemas, escalamiento de privilegios, análisis forense y uso de herramientas especializadas como Metasploit, SIEM, firewalls y benchmarks de seguridad. Estas actividades son fundamentales para el aprendizaje activo y el desarrollo de competencias profesionales de ciberseguridad.

El profesional de ciberseguridad debe contar con conocimientos técnicos, legales y éticos. No basta con saber cómo atacar o defender, sino también comprender el por qué y el hasta dónde de cada acción. Solo así se evita la ejecución de prácticas abusivas, se protege la privacidad de los usuarios. Si se garantiza una actuación profesional responsable en entornos organizacionales.

Recomendaciones

Establecer rutinas de simulación ofensiva y defensiva en ambientes controlados que permitan evaluar el nivel real de exposición frente a amenazas informáticas. Estos ejercicios deben estar documentados, aprobados éticamente y alineados con el marco legal vigente.

Aplicar buenas prácticas de configuración segura, gestión de accesos, monitoreo y hardenización de sistemas basadas en estándares reconocidos como los CIS Benchmarks. Esto contribuye a prevenir vulnerabilidades ya conocidas y a fortalecer la seguridad desde una perspectiva técnica y normativa.

Desarrollar políticas internas de ciberseguridad y códigos de ética profesional, incluyendo protocolos de denuncia y mecanismos de supervisión que garanticen la actuación de los colaboradores bajo principios de integridad, legalidad y transparencia.

Capacitar de forma continua al personal técnico y administrativo, no solo en herramientas y metodologías de ciberseguridad, sino también en normativas legales, ética profesional, tratamiento de datos personales, respuesta ante incidentes y análisis forense. Esta formación debe contemplar tanto marcos nacionales como internacionales.

Implementar herramientas de código abierto o soluciones gratuitas como Wazuh, pfSense u OSSIM Que permitan a las organizaciones con presupuestos limitados a aplicar controles efectivos de seguridad, detección de intrusos, segmentación de redes y análisis de eventos sin incurrir en altos costos.

Referencias Bibliográficas

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

Chindrus, C., & Caruntu, C.-F. (2023). Securing the network: A red and blue cybersecurity competition case study. Information, 14(11), 587. https://doi.org/10.3390/info14110587

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

Congreso Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso Colombia. (2009). Ley 1273 [LEY_1273_2009] (pp. 1–4). https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

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

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495): Seguridad en IPv6 (pp. 10–29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

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

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

MINTIC. (2022). Políticas de privacidad y condiciones de uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

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

OAS. (2018). Convenio sobre la ciberdelincuencia (pp. 3–26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

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

Quintero, J. (2020). RedTeam y BlueTeam, equipos estratégicos al interior de una organización [Objeto virtual de información - OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/35497

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

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

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework. Revista Seguridad UNAM. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Zambrano Hernández, M., Peña Hidalgo, H. J., & Cárdenas Corral, J. (2024). Guía para la gestión y clasificación de incidentes de ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus, D. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia. Repositorio UNAD. https://repository.unad.edu.co/handle/10596/17410