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

Jarvin Daniel Navas Prieto

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2026

Dedicatoria

Quiero ofrecer todo este esfuerzo, dedicación y trabajo a Dios y a mi familia, quienes, a pesar de las dificultades, siempre han estado presentes apoyándome en este largo camino lleno de obstáculos. A mi esposa, por su apoyo incondicional desde el primer momento en que decidí estudiar; asumimos este reto ya casado y con un hijo en camino, siendo ella mi mayor motor y el pilar para no desfallecer ante las frustraciones académicas, laborales y cotidianas. A mis dos hermosos hijos, porque a pesar de su corta edad, entienden con mucho amor los sacrificios que he hecho para darles un mejor futuro.

A mis padres, porque, aunque la vida no nos dio la oportunidad de estudiar en su momento por situaciones económicas, siempre me apoyaron de una u otra forma, lo cual vale más que cualquier cosa.

En general, a toda mi familia cercana, quienes nunca dudaron de mí y hoy se sienten orgullosos de tener al primer Ingeniero de la familia y, próximamente, al primer Especialista.

Y finalmente, a quienes no creyeron en mí: a ellos también les dedico este logro, porque lejos de ser un obstáculo, se convirtieron en la inspiración para demostrarme de qué soy capaz.

Agradecimientos

Agradezco de manera muy especial a la Universidad Nacional Abierta y a Distancia (UNAD), ya que, gracias a su metodología y modalidad de estudio, tuve la oportunidad de iniciar mi carrera profesional, culminarla con éxito y, ahora, estar a las puertas de alcanzar mi especialización.

A los docentes y tutores, por compartir sus conocimientos con paciencia, exigencia y dedicación, guiándome con éxito en el desarrollo de este trabajo y a lo largo de mi formación.

Finalmente, agradezco nuevamente a Dios por todas las bendiciones brindadas durante estos seis años de trayectoria académica; sin su fortaleza y guía, nada de esto hubiera sido posible.

Resumen

Este documento expone la aplicación práctica de estrategias de ciberseguridad ofensiva y defensiva sobre la infraestructura corporativa de SecureNova Labs. El ejercicio se fundamenta en un análisis normativo regido por las leyes 1273 de 2009 y 1581 de 2012 en Colombia, garantizando el rigor ético y legal de la auditoría. Durante la fase ofensiva, se ejecutó una prueba de penetración que evidenció la explotación activa de la vulnerabilidad MS17-010 (EternalBlue) a través de servicios SMBv1 desactualizados, lo que permitió el compromiso del sistema. Posteriormente, desde el enfoque defensivo, se estructuró una propuesta de contención e implementación de herramientas de monitoreo continuo de código abierto, específicamente Wazuh y Suricata. Asimismo, se establecieron directrices de endurecimiento (hardening) basadas en los controles de CIS Benchmarks para fortalecer la arquitectura de red y mitigar la recurrencia de incidentes.

Palabras clave: ciberseguridad, contención, explotación, pentesting, vulnerabilidad

Abstract

This paper presents the practical application of offensive and defensive cybersecurity strategies on the corporate infrastructure of SecureNova Labs. The study is grounded in a regulatory analysis governed by Colombian Laws 1273 of 2009 and 1581 of 2012, ensuring the ethical and legal compliance of the audit. During the offensive phase, a penetration test was executed, demonstrating the active exploitation of the MS17-010 (EternalBlue) vulnerability through outdated SMBv1 services, which led to system compromise. Subsequently, from a defensive perspective, a containment proposal was structured, including the implementation of open-source continuous monitoring tools, specifically Wazuh and Suricata. Furthermore, hardening guidelines based on CIS Benchmarks controls were established to strengthen the network architecture and mitigate the recurrence of security incidents.

Keywords: containment, cybersecurity, exploitation, pentesting, vulnerability.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Para garantizar la precisión conceptual de este informe, las siguientes definiciones se alinean con la terminología estandarizada de ciberseguridad **(INCIBE, 2021)**:

Blue Team:

Equipo de profesionales de seguridad de carácter proactivo y preventivo, encargado de defender, monitorear y mejorar las configuraciones de la infraestructura de una organización de forma continua.

Ciberespionaje:

Actividad ilícita orientada a obtener secretos, información confidencial o datos sensibles sin autorización, utilizando técnicas de infiltración en redes informáticas.

CIS Benchmarks:

Guías y estándares de mejores prácticas reconocidas a nivel mundial para la configuración segura de sistemas operativos, software y redes.

EternalBlue (MS17-010):

Vulnerabilidad crítica de ejecución remota de código (RCE) en el protocolo SMBv1 de Microsoft Windows, utilizada para corromper la memoria y obtener privilegios de sistema.

Hardenización (Hardening):

Proceso de aseguramiento de un sistema operativo o red mediante la reducción de su superficie de ataque, eliminando privilegios o desactivando protocolos heredados.

Pentesting:

Prueba de penetración metodológica y controlada (compuesta por reconocimiento, escaneo, explotación y reporte) para evaluar la seguridad de una infraestructura TI.

Pivoting (Movimiento Lateral):

Técnica utilizada por atacantes para emplear una máquina ya comprometida dentro de una red como vector o puente para acceder a otros segmentos o servidores internos.

Red Team:

Equipo de expertos en ciberseguridad ofensiva que emula las tácticas, técnicas y procedimientos de atacantes reales para identificar vulnerabilidades explotables en una organización.

Reverse Shell (Shell Inversa):

Carga útil (payload) inyectada en un servidor víctima que fuerza a dicho servidor a iniciar una conexión de vuelta hacia la máquina del atacante para otorgarle una consola de administración remota.

SIEM (Security Information and Event Management):

Herramienta centralizada que recolecta, normaliza y correlaciona registros (logs) en tiempo real para identificar anomalías y generar alertas tempranas.

Introducción

En el entorno corporativo contemporáneo, las organizaciones enfrentan un panorama de amenazas cibernéticas caracterizado por vectores de ataque de complejidad incremental y para hacerles frente se necesita una respuesta técnica muy bien coordinada entre los equipos defensivos y ofensivos (Angarita Carrascal, 2021; Dominguez Sierra, 2020; Medina Beltran, 2023). Sin embargo, el despliegue de capacidades técnicas para la defensa o auditoría de sistemas carece de validez si se omiten los principios éticos y el marco legal vigente

El presente documento consolida los hallazgos y las estrategias diseñadas a partir de la simulación de un incidente real dentro de la red corporativa de SecureNova Labs. El documento se encuentra estructurado de manera secuencial. Se inicia con una revisión de la legislación aplicable en Colombia con el propósito de delimitar los alcances éticos y normativos de la investigación

Tras delimitar los alcances éticos y normativos acordados, se procede con la documentación de las operaciones ofensivas desde la visión del Red Team. En esta sección se demostró la viabilidad de vulnerar la red desde un vector externo, aprovechando la conocida falla MS17-010 para entrar y ejecutar movimientos laterales manteniendo el alcance dentro del entorno de pruebas.

Posterior a la ejecución ofensiva, se iniciaron las labores de mitigación. En la sección final del informe se aborda la perspectiva defensiva desde el rol del Blue Team. En dicho apartado se detalla la transición del monitoreo pasivo de alertas a la contención activa de intrusiones en tiempo real. Para lograrlo, se justifica el uso de herramientas de código abierto (GPL) y la adopción de estándares de seguridad internacionales, buscando que la infraestructura de la empresa quede realmente sólida frente a un ataque verdadero.

Justificación

La justificación de esta auditoría se fundamenta en la necesidad imperativa de que las organizaciones identifiquen y mitiguen proactivamente sus vulnerabilidades antes de que sean explotadas por un actor de amenaza externo. El ejercicio realizado en SecureNova Labs es un ejemplo claro de esto, ya que demuestra cómo la falta de parches de seguridad y el uso de protocolos obsoletos terminan abriendo brechas críticas en la infraestructura tecnológica. La ejecución de auditorías de seguridad y la búsqueda activa de vulnerabilidades conllevan riesgos inherentes. La omisión de lineamientos éticos durante esta labor puede exponer tanto a la organización como al auditor a graves implicaciones legales y reputacionales.

Por otro lado, el documento también sirve para demostrar que la verdadera ciberseguridad es un trabajo en equipo. La identificación de vectores de ataque y el análisis de impacto por parte del Red Team carecen de efectividad si no se cuenta de manera simultánea con un Blue Team capacitado para mitigar brechas, aislar activos afectados e implementar directrices de endurecimiento (hardening) de manera oportuna

Por último, el ejercicio demuestra que el aseguramiento de la infraestructura corporativa no depende exclusivamente de presupuestos elevados. Se concluye que la adopción de metodologías estructuradas y el aprovechamiento de soluciones de código abierto facilitan el diseño de una arquitectura de defensa robusta.

Objetivos

Objetivo General

Diseñar un marco metodológico de defensa y contención para la infraestructura tecnológica de SecureNova Labs, mediante la evaluación cuantitativa de vulnerabilidades técnicas y la alineación con la legislación colombiana vigente, con el propósito de mitigar intrusiones informáticas garantizando el estricto cumplimiento normativo.

Objetivos Específicos

Ejecutar pruebas controladas de reconocimiento, explotación y movimiento lateral (pivoting) en un entorno de laboratorio, con el fin de mapear los vectores de ataque orientados al compromiso de la infraestructura.

Estructurar una guía de respuesta a incidentes enfocada en la contención inmediata de amenazas, el aislamiento lógico de los nodos comprometidos y la preservación de la evidencia digital.

Establecer configuraciones de endurecimiento (hardening) basadas en los estándares CIS Benchmarks y proponer la implementación de sistemas de monitoreo continuo (SIEM e IPS) para garantizar la visibilidad y mitigar futuras brechas.

Marco Normativo, Ético y Entorno de Ciberseguridad

La auditoría de sistemas y la simulación de adversarios no ocurren en un vacío técnico; operan dentro de un ecosistema complejo donde convergen el riesgo corporativo, la responsabilidad civil y el derecho penal. El desarrollo de habilidades ofensivas (Red Team) y defensivas (Blue Team) exige que el profesional comprenda las fronteras legales de su actuar. En este capítulo se establece el marco normativo y ético que rige las operaciones de ciberseguridad en Colombia, delimitando las líneas rojas entre el hacking ético autorizado y el cibercrimen, tomando como base de análisis crítico el entorno corporativo propuesto por SecureNova Labs.

Legislación Colombiana en el Contexto de la Ciberseguridad

En el ámbito de la ciberseguridad corporativa, la destreza técnica carece de valor —y se convierte en un riesgo inminente para el profesional y la organización— si no está estrictamente alineada con el marco legal vigente. En Colombia, la actuación de los equipos estratégicos está regulada principalmente por dos frentes normativos interconectados: la penalización estricta de los delitos informáticos y la protección de los datos personales.

Por un lado, la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009) se erige como la "regla de oro" y el pilar fundamental en la legislación nacional para la ciberseguridad. Esta normativa modificó el Código Penal colombiano para crear un nuevo bien jurídico tutelado: la protección de la información y de los datos. Su implementación dotó a la justicia de las herramientas necesarias para judicializar acciones que, por su naturaleza técnica, son exactamente las mismas que utiliza un Red Team durante una auditoría (Guarnizo Portela, 2024): acceso a sistemas mediante exploits, interceptación de tráfico de red, y ejecución de software diseñado para escalar privilegios.

Para un auditor de ciberseguridad, esta ley define la línea divisoria absoluta de la legalidad. Operar sin un documento de Reglas de Enfrentamiento (RoE - Rules of Engagement) explícitamente firmado por el representante legal de la empresa auditada convierte inmediatamente una prueba de penetración en un conjunto de delitos tipificados. El RoE y los Acuerdos de Nivel de Servicio (SLA) actúan como la cláusula de exención de responsabilidad, autorizando las pruebas de estrés sobre la infraestructura bajo parámetros estrictamente delimitados.

Por otro lado, la Ley Estatutaria 1581 de 2012 (Congreso de la República de Colombia, 2012) regula el derecho constitucional al Habeas Data. Esta norma establece que ninguna entidad o individuo puede recolectar, almacenar, usar o compartir datos personales sin la autorización expresa, clara y previa del titular. En el contexto del pentesting, esto impacta directamente las fases de post-explotación y exfiltración de datos. Si un Red Team logra vulnerar un servidor de bases de datos, la simple visualización, extracción o copia de esos registros en texto claro constituye una violación a esta ley. Esto exige la implementación de protocolos estrictos de manejo de evidencias por parte de la firma auditora. El cumplimiento operativo de esta ley y sus lineamientos diarios fueron reglamentados posteriormente por el Decreto 1377 de 2013 (Presidencia de la República de Colombia, 2013).

Análisis Ético y Legal: Caso de Estudio "SecureNova Labs"

Para ilustrar la fricción del mundo real que puede existir entre las exigencias corporativas desreguladas y la legalidad, se analizó a profundidad el escenario del Acuerdo de Confidencialidad (NDA) propuesto por la firma internacional SecureNova Labs para sus nuevos integrantes de los equipos Red y Blue Team.

Al evaluar dicho documento bajo la lupa de la legislación penal colombiana, se evidencian múltiples cláusulas que resultan nulas de pleno derecho. El principio fundamental del derecho laboral y comercial establece que ningún contrato puede obligar a un profesional a cometer un delito, a encubrirlo, o a renunciar a sus derechos fundamentales. Las irregularidades más críticas detectadas en este acuerdo incluyen:

- **Disfraz de delitos como secreto industrial**: En la segunda cláusula, el acuerdo clasifica de manera anómala como "información confidencial" a los datos provenientes de interceptaciones ilegales (conocidas popularmente como "chuzadas") y accesos abusivos a sistemas informáticos. Un secreto industrial protege la propiedad intelectual legítima, no el producto de la vulneración sistemática de sistemas de terceros. Esta estipulación viola flagrantemente el Artículo 269A (Acceso abusivo a un sistema informático) y el Artículo 269C (Interceptación de datos informáticos) de la Ley 1273 de 2009.
- **Obligación de complicidad y omisión de denuncia:** La cuarta cláusula actúa como una mordaza legal, prohibiendo expresamente al empleado denunciar ante las autoridades cualquier "actividad sospechosa de espionaje" y restringiendo la divulgación de información ilegal a terceros. Esta exigencia atenta contra la integridad profesional e induce directamente al trabajador a cometer el delito de

omisión de denuncia. En la jurisprudencia, procesar datos a sabiendas de su origen ilícito transforma al ingeniero de un simple empleado a un cómplice o coautor de los delitos informáticos de la organización, incurriendo además en el delito de receptación.

- **Traslado de responsabilidad penal (Estrategia de escudo humano):** La octava cláusula exige que, en caso de un allanamiento judicial o investigación, el empleado debe asumir su propia defensa legal y garantizar que SecureNova Labs quede totalmente eximida de culpa. Esta es una maniobra corporativa abusiva para evadir la responsabilidad penal y utilizar al personal técnico como barrera de contención o "escudo humano" frente al aparato de justicia.

A pesar de que ofertas de este tipo estén acompañadas de condiciones económicas excepcionalmente atractivas —tales como salarios de $15.000.000 COP mensuales y contratos laborales de carácter vitalicio—, la aceptación de estas condiciones es insostenible y destructiva desde el punto de vista ético y legal.

El Consejo Profesional Nacional de Ingeniería (COPNIA, 2015) es imperativo en su Código de Ética: el ejercicio de la ingeniería en Colombia debe estar siempre al servicio de la legalidad, la honestidad y la protección de la sociedad. Firmar un acuerdo de la naturaleza propuesta por SecureNova Labs expondría al profesional no solo a penas privativas de la libertad en centros carcelarios, sino a una investigación disciplinaria que culminaría con la cancelación definitiva de su matrícula profesional por parte del Tribunal de Ética, inhabilitándolo de por vida para ejercer la profesión.

Políticas de Acceso y Supervisión para Firmas Auditoras

La auditoría de sistemas requiere que un tercero evalúe las debilidades internas, lo que inherentemente genera un riesgo de exposición de la información corporativa. Para evitar que las empresas de ciberseguridad contratadas exploten indebidamente la información sensible de sus clientes durante una prueba de penetración, es imperativo abandonar los modelos tradicionales de confianza implícita.

Las operaciones de ciberseguridad deben regirse estrictamente por la arquitectura de Confianza Cero (Zero Trust) y el Principio de Mínimo Privilegio (PoLP). Las firmas auditoras solo deben poseer accesos efímeros y altamente controlados a los perímetros estrictamente acordados en los Acuerdos de Nivel de Servicio (SLA). Para garantizar la transparencia y proteger los activos organizacionales, el Blue Team interno debe implementar las siguientes medidas de control tecnológico:

- **Enmascaramiento y Tokenización de Datos (Data Masking):** Se deben utilizar técnicas de ofuscación de bases de datos de pre-producción. Esto garantiza que, si el Red Team logra explotar una vulnerabilidad y acceder a la base de datos, interactúe únicamente con registros anonimizados o datos sintéticos (dummy data), previniendo la exposición de Información Personal Identificable (PII) de los clientes reales.
- **Monitoreo Activo (Auditoría al Auditor):** La confianza no excluye el control. El Blue Team interno debe auditar continuamente el comportamiento de la firma externa. A nivel técnico, esto requiere la implementación de soluciones SIEM para ingerir, registrar y correlacionar cada comando ejecutado, cada intento de escalamiento de privilegios y cada paquete anómalo enviado por los auditores dentro de la ventana de pruebas.

- **Entornos Controlados y Micro-segmentación (Sandboxing):** Se debe aplicar la regla de las dos personas para autorizar accesos a segmentos críticos. Las pruebas ofensivas deben ejecutarse en infraestructuras virtualizadas y altamente segmentadas (como entornos controlados en VirtualBox o redes VLAN aisladas). Esto asegura que el uso de herramientas forenses de análisis profundo o la inyección de payloads no dejen puertas traseras (persistencia) ni permitan la exfiltración de información confidencial hacia servidores externos no autorizados.

Respuesta a Incidentes de Ciberespionaje Corporativo

En el eventual caso de que los sistemas de monitoreo defensivo detecten actos de ciberespionaje, robo de propiedad intelectual o exfiltración maliciosa por parte de una firma contratista, el plan de respuesta a incidentes de la organización debe ser fulminante e implacable.

A nivel técnico, se debe ejecutar la desconexión y revocación inmediata de todas las credenciales y accesos VPN proporcionados a la firma. A nivel legal, se debe solicitar el embargo preventivo de los equipos informáticos del contratista (mediante orden judicial) para garantizar la cadena de custodia de la evidencia digital, procediendo con la respectiva denuncia penal y demandas civiles por daños y perjuicios. Para restaurar la confianza operativa de la empresa vulnerada, será obligatorio contratar una firma auditora independiente que realice un peritaje forense exhaustivo, publique informes de transparencia para los accionistas y reestructure integralmente el Sistema de Gestión de Seguridad de la Información (SGSI) bajo estándares internacionales como la ISO 27001.

Operaciones Ofensivas y Simulación de Amenazas (Red Team)

La simulación de adversarios (Red Teaming) constituye un procedimiento esencial para evaluar la resiliencia operativa de la infraestructura. Ejecutar un análisis automatizado de vulnerabilidades, una verdadera prueba de penetración sigue un orden estricto. El ejercicio se fundamenta en el estándar internacional PTES con el objetivo de emular las tácticas, técnicas y procedimientos de un actor de amenazas avanzado.

Este capítulo detalla los procedimientos de intrusión ejecutados sobre la red corporativa de SecureNova Labs.Fases metodológicas de la prueba

Previo a la ejecución del vector ofensivo, se estructuró la planificación estratégica de la auditoría. Un pentesting profesional requiere la ejecución rigurosa y estructurada de metodologías estandarizadas (INCIBE, 2019; Sello Editorial UNAD, 2024; Zuluaga Mateus, 2017). Para este estudio, la operación se estructuró en seis fases metodológicas estandarizadas:

Reconocimiento: Consiste en la recopilación pasiva de información sobre el objetivo sin interactuar directamente con sus sistemas para mitigar su detección, empleando herramientas de inteligencia de fuentes abiertas (OSINT) como Maltego.

Escaneo y enumeración: Implica la interacción activa con la infraestructura para identificar puertos abiertos y los sistemas operativos en ejecución. La herramienta clave en este punto fue Nmap.

Análisis de vulnerabilidades: Se contrastó la información de los servicios identificados con bases de datos públicas como ExploitDB. Para optimizar el proceso, se emplearon escáneres automatizados de código abierto como OpenVAS.

Explotación: Constituye la materialización de la intrusión. Se aprovecharon las vulnerabilidades identificadas previamente para el envío de cargas útiles (payloads), con el fin de

comprometer y obtener acceso inicial al sistema. Para esto, Metasploit es el estándar por excelencia.

Post-explotación: Tras obtener el acceso inicial, se procede a garantizar la persistencia en el sistema. El objetivo de esta fase consiste en escalar privilegios y extraer información sensible. Un procedimiento estándar implica el uso de herramientas como Mimikatz para la extracción de credenciales residentes en memoria.

Reporte: Finalmente, es necesario documentar todos los vectores de ataque explotados con éxito y proponer soluciones técnicas de seguridad (hardening) para su remediación, apoyándose en plataformas de gestión como Dradis.

Preparación del entorno y reconocimiento inicial (Capa 2 del modelo OSI)

La estación de ataque se consolidó mediante la distribución Parrot OS Security, que es un sistema basado en Debian y cuenta con las herramientas preinstaladas requeridas para la ejecución de auditorías de seguridad. La fase inicial consistió en el mapeo de la red local para identificar los objetivos potenciales, con el objetivo de evadir las alertas de los sistemas de detección (IPS) de la empresa antes de tiempo.

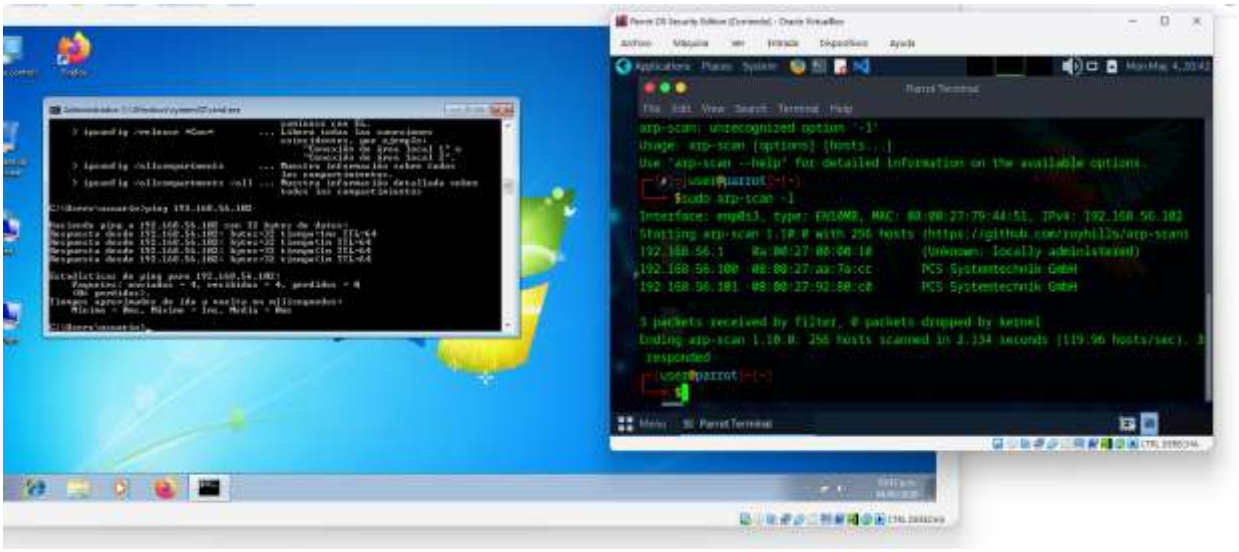
Para identificar los dispositivos conectados en el segmento con el fin de mitigar la generación de alertas en los enrutadores, se ejecutó un barrido utilizando el protocolo ARP. La elección del protocolo ARP frente a solicitudes ICMP (ping) se fundamenta en que el protocolo ICMP opera en la capa 3 y los cortafuegos modernos restringen este tipo de tráfico. ARP, en cambio, trabaja más abajo, directamente en la capa 2 (Capa de Enlace de Datos).

Mediante el despliegue de la herramienta arp-scan, se solicitaron de forma imperativa las respuestas de las interfaces de red del segmento con sus direcciones IP y MAC, independientemente de las reglas establecidas en el cortafuegos interno. Gracias a este escaneo

se identificaron dos hosts activos: uno con la IP 192.168.56.100 y otro con la 192.168.56.101. Además, con solo revisar los primeros números de las direcciones MAC (el identificador OUI), se confirmó de inmediato que los objetivos correspondían a máquinas virtuales ejecutadas en VirtualBox.

Figura 1

Reconocimiento de IPs



Nota. Resultados del escaneo de red en capa 2 utilizando la herramienta arp-scan para identificar las direcciones IP y MAC de las máquinas virtuales activas en el entorno de laboratorio

El arsenal ofensivo (Herramientas y OSINT)

La ejecución práctica de la auditoría técnica requiere el despliegue de herramientas especializadas. La efectividad de las operaciones ofensivas está supeditada al arsenal técnico disponible. Las herramientas seleccionadas para ejecutar la auditoría sobre la red de SecureNova Labs fueron las siguientes:

Metasploit Framework: Entorno de trabajo estándar para la explotación de vulnerabilidades. Desarrollado en Ruby, permitió centralizar la operación, configurar las cargas

maliciosas (payloads) y administrar el sistema comprometido de manera remota mediante la consola de Meterpreter.

Nmap: Motor principal utilizado para el escaneo de la red a bajo nivel. Permitió la identificación de equipos activos en la red, qué puertos tenían abiertos y, usando sus scripts internos (NSE), se detectaron fallas específicas en servicios como SMB sin necesidad de lanzar un ataque directo de inmediato.

OpenVAS: Utilizado como escáner automatizado de vulnerabilidades. Su función consistió en contrastar los servicios detectados en la red contra una base de datos de fallos conocidos (CVE), generando un mapa de riesgo inicial exhaustivo.

CVE y ExploitDB: El análisis requirió la consulta obligatoria del código universal de las fallas (los identificadores CVE). En conjunto con este procedimiento, se empleó ExploitDB, que es la biblioteca pública donde los investigadores suben el código exacto (las Pruebas de Concepto o PoC) requeridas para la inyección en Metasploit y el posterior compromiso del sistema.

Alineación ética y legal (Reglas de Enfrentamiento)

Antes de lanzar un solo escaneo contra las IPs 192.168.56.100 y 192.168.56.101, se establecieron formalmente las Reglas de Enfrentamiento (RoE). Considerando los lineamientos éticos y legales, la ejecución de escaneos activos sin autorización previa constituye una conducta penalizable bajo el Artículo 269A de la Ley 1273 de 2009.

Por eso, todo lo que documentamos en este informe parte de un escenario donde ya existía un acuerdo firmado (SLA) con la gerencia de SecureNova Labs. La gerencia de SecureNova Labs otorgó una ventana de tiempo específica y la autorización formal para el despliegue de herramientas ofensivas. Además, para respetar la Ley de Protección de Datos

(1581 de 2012) y el Código de Ética del COPNIA, se estableció que, en caso de vulnerar el sistema exitosamente, no se procedería con la exfiltración o descarga de bases de datos de producción. Se acordó evidenciar el control administrativo... garantizando una prueba de penetración ética, demostrable y sin afectación a la disponibilidad de los activos.

Armado del laboratorio y solución de problemas (Troubleshooting)

Con el fin de evitar impactos en la infraestructura de la empresa en la vida real, se estructuró un laboratorio de pruebas aislando todo dentro del hipervisor Oracle VirtualBox. Se configuró una estación de ataque ejecutando Parrot OS (Debian 12) y una máquina víctima con Windows 7 Professional.

Como es normal al importar máquinas virtuales (los archivos .ova), se presentaron incompatibilidades técnicas que requirieron la aplicación de procesos de troubleshooting sobre la marcha para poder continuar:

Falla con los puertos USB: El hipervisor desplegó un error por conflicto de nombres (error VERR_PDM_USB_NAME_CLASH) y no dejaba arrancar la máquina. El archivo contenía una configuración de controladores USB incompatible con el hardware físico subyacente. Se accedió a los ajustes de la máquina virtual para desactivar de manera imperativa el controlador USB

Error de NVRAM: El sistema arrojó un mensaje de error indicando la ausencia de la ruta de almacenamiento NVRAM. Esta condición se originó por la desincronización de la máquina con el modo de arranque (EFI). La solución fue ir a la configuración de la placa base virtual, desactivar la casilla de UEFI, volverla a marcar, lo cual permitió la regeneración del sector de arranque por parte del hipervisor.

Permisos al hacer Ping: Al intentar enviar paquetes ICMP (ping) desde el equipo atacante hacia la red local, el sistema operativo arrojó un error de permisos. Este comportamiento es característico de las restricciones de seguridad en sistemas basados en Linux: para abrir conexiones de red a bajo nivel (sockets crudos) se necesita ser administrador. La anteposición del comando de superusuario (sudo) otorgó los privilegios requeridos para la apertura de sockets crudos, normalizando el tráfico de red.

Escaneo, enumeración y análisis de vulnerabilidades

Ya con el laboratorio sin errores, se procedió al uso de Nmap para escanear los puertos y reconocer la topología del entorno evaluado.

Durante el análisis del primer objetivo (IP 192.168.56.100), se identificó que la totalidad de sus 65.535 puertos se encontraban cerrados u omitiendo las peticiones de red entrantes. Al no tener nada expuesto, se determinó que el activo corresponde a infraestructura interna restrictiva, probablemente desempeñando funciones de servidor DHCP en la red.

En contraste, el análisis de la segunda IP (192.168.56.101, Host-A) arrojó resultados diferentes. Se ejecutó un escaneo exhaustivo (sudo nmap -sV -sC -p-) para identificar de manera forzada las versiones exactas de los servicios en ejecución.

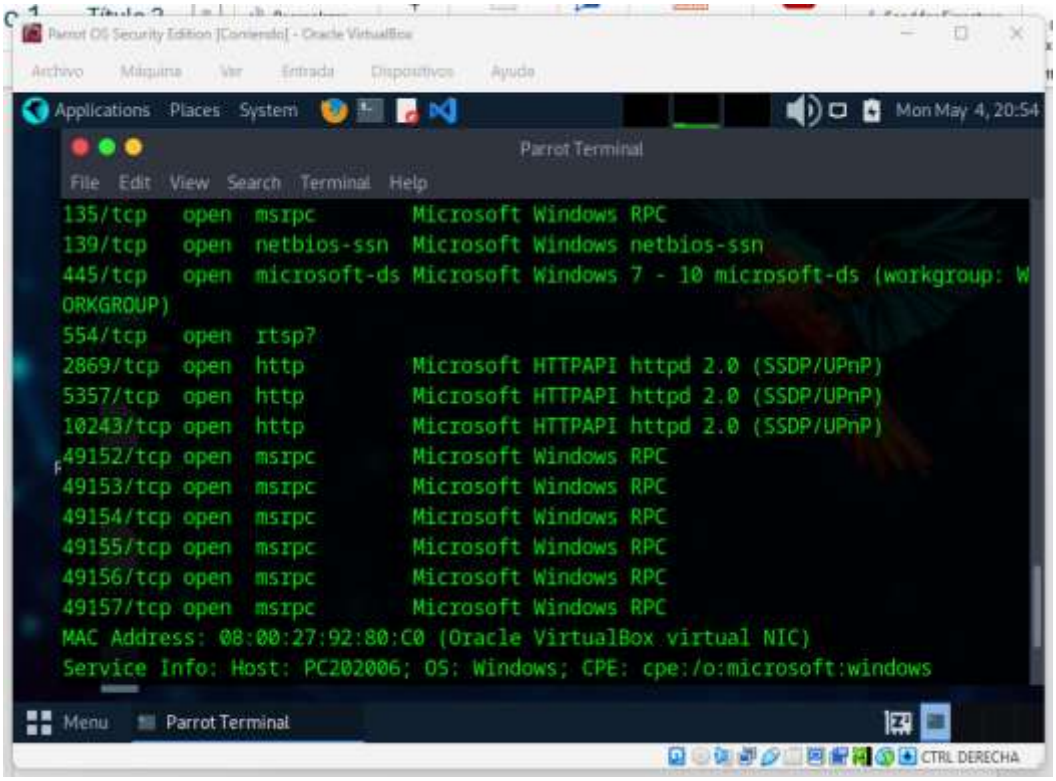
Ese puerto le pertenece al protocolo SMB en su versión 1, el cual sirve para compartir archivos e impresoras en Windows. A nivel de seguridad informática, el protocolo SMBv1 posee fallos de diseño críticos en la gestión de memoria, siendo la puerta de entrada más común para comprometer infraestructuras corporativas.

Para confirmar la vulnerabilidad sin ejecutar la carga útil maliciosa, se procedió a emplear scripts del motor NSE de Nmap (--script smb-vuln*). La función de este script es enviar paquetes específicos al sistema operativo Windows para evaluar su respuesta y determinar su

estado de actualización. El resultado confirmó que el Host-A carecía de las actualizaciones: el Host-A no tenía los parches de seguridad de Microsoft y era altamente vulnerable a la falla MS17-010, mejor conocida en el mundo como EternalBlue.

Figura 2

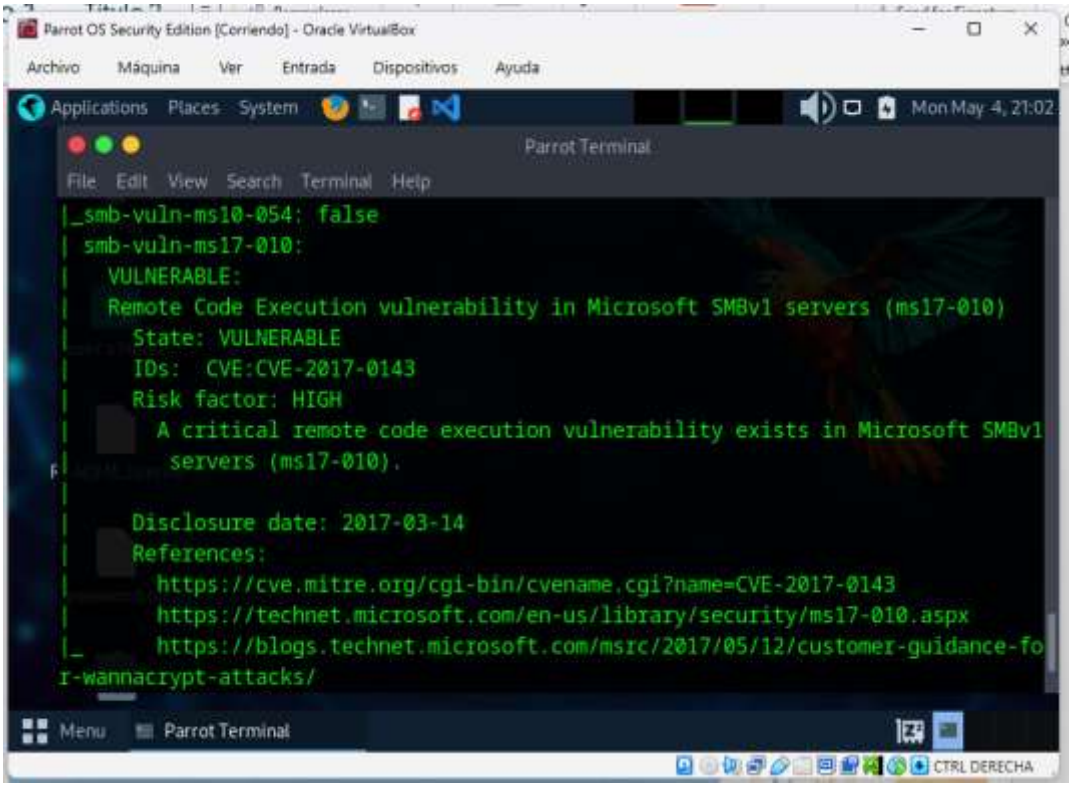
Revisión de puertos abiertos



Nota. Salida del escaneo de puertos ejecutado con Nmap, evidenciando la exposición del puerto 445 correspondiente al servicio SMBv1 en la máquina objetivo.

Figura 3

Revisión Vulnerabilidades CVE-2017-0143



Nota. Confirmación de la vulnerabilidad CVE-2017-0143 (MS17-010) mediante el uso de los scripts de enumeración de vulnerabilidades (NSE) nativos de Nmap.

Ficha técnica y análisis CVSS de la falla

Antes de lanzar el ataque definitivo (fase de weaponization), se procedió a documentar la severidad de la vulnerabilidad identificada. Con el fin de cuantificar el impacto técnico y operacional para la alta gerencia, se aplicó la métrica estándar internacional CVSS (versión 3.1).

- **Identificador CVE:** CVE-2017-0143
- **Nombre común:** MS17-010 o EternalBlue (Microsoft, 2017)
- **Vector CVSS:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Impacto técnico de la vulnerabilidad:** Esta falla corresponde a una vulnerabilidad de Ejecución Remota de Código (RCE). La vulnerabilidad radica en el núcleo de Windows, específicamente en el archivo srv.sys que maneja el SMBv1. Al procesar una solicitud estructurada del tipo SrvOs2FeaToNt, el sistema omite la validación de límites de memoria, lo que causa un desbordamiento de búfer. Esta condición facilita la sobreescritura del área de memoria non-paged pool sin autenticación previa, posibilitando la inyección y ejecución de código arbitrario con privilegios elevados de SYSTEM

Tabla 1

Descripción técnica de la vulnerabilidad (Análisis CVSS v3.1)

Criterio	Nivel	Explicación Práctica
Puntuación Base	8.1 (Alto) a 9.3 (Crítico)	Varía un poco dependiendo del vector de red exacto.
Vector de Ataque (AV)	Red	Se puede atacar por internet o por red local; No requiere acceso físico al dispositivo.
Complejidad (AC)	Alta	Requiere ciertos conocimientos técnicos para saber cómo corromper la memoria sin dañar el equipo.
Privilegios (PR)	Ninguno	No requiere autenticación ni conocimiento previo de credenciales.
Interacción (UI)	Ninguna	El ataque es "Zero-Click". El usuario no tiene que abrir ningún correo ni descargar nada.
Confidencialidad (C)	Alto	Permite la lectura de cualquier archivo del sistema.

Integridad (I)	Alto	Facilita la modificación, eliminación o alteración cualquier archivo a nuestro antojo.
Disponibilidad (A)	Alto	Otorga la capacidad de desplegar ataques tipo Ransomware y secuestrar la red (como pasó con el virus WannaCry).

Nota. Esta tabla detalla la evaluación de los criterios del estándar CVSS v3.1 utilizados para clasificar el nivel de criticidad de la vulnerabilidad MS17-010.

Modelado de la amenaza: Cyber Kill Chain

Para evaluar el flujo del compromiso en SecureNova Labs, las acciones ofensivas se mapearon conforme al modelo Cyber Kill Chain de Lockheed Martin (2015). Este modelo divide un ataque en siete etapas secuenciales; la detección oportuna en cualquiera de estos eslabones interrumpe la cadena de intrusión. La ventaja estratégica de este modelo radica en que la interrupción táctica en cualquiera de los eslabones secuenciales neutraliza por completo la intrusión.

El flujo de la intrusión se estructuró de la siguiente manera:

1. **Reconocimiento:** Esta etapa contempló la ejecución de las herramientas arp-scan y Nmap. Se identificó la dirección IP del host objetivo, determinando el uso del sistema operativo Windows 7 y la exposición del puerto 445, evitando la escritura en disco para evadir las firmas del software antivirus
2. **Preparación (*Weaponization*):** Se procedió con la vectorización del ataque o ensamblaje de la carga útil (Weaponization).

3. **Entrega:** Transmisión del exploit a través del segmento de red local mediante paquetes malformados dirigidos al puerto 445/TCP, requiriendo cero interacciones por parte del usuario objetivo
4. **Explotación:** utilizar Nmap para el escaneo de puertos y el reconocimiento del entorno objetivo en el archivo srv.sys y corrompió la memoria RAM del sistema.
5. **Instalación:** El vector operó bajo la modalidad de amenaza residente en memoria (Fileless). El código malicioso se ejecutó directamente en la memoria RAM sin realizar escrituras en el almacenamiento físico, evadiendo la detección basada en firmas estáticas del software antivirus.
6. **Comando y Control (C2):** La máquina objetivo estableció una conexión de retorno hacia la estación de ataque (IP 192.168.56.102) por el puerto 4444, estableciendo una interfaz de línea de comandos remota.
7. **Acciones sobre el objetivo:** Tras consolidar el control total con privilegios de NT AUTHORITY\SYSTEM, se inició la fase de pivotaje técnico de red y se procedió a la creación de una cuenta de usuario llamado "JarvinNavas" con permisos de administrador.

Explotación de la infraestructura (MS17-010)

Con la vulnerabilidad confirmada, se inicializó el framework Metasploit (msfconsole), cargando el módulo específico exploit/windows/smb/ms17_010_eternalblue.

Se procedió con la parametrización de las variables de red del host remoto (RHOST) y del host de escucha local (LHOST).

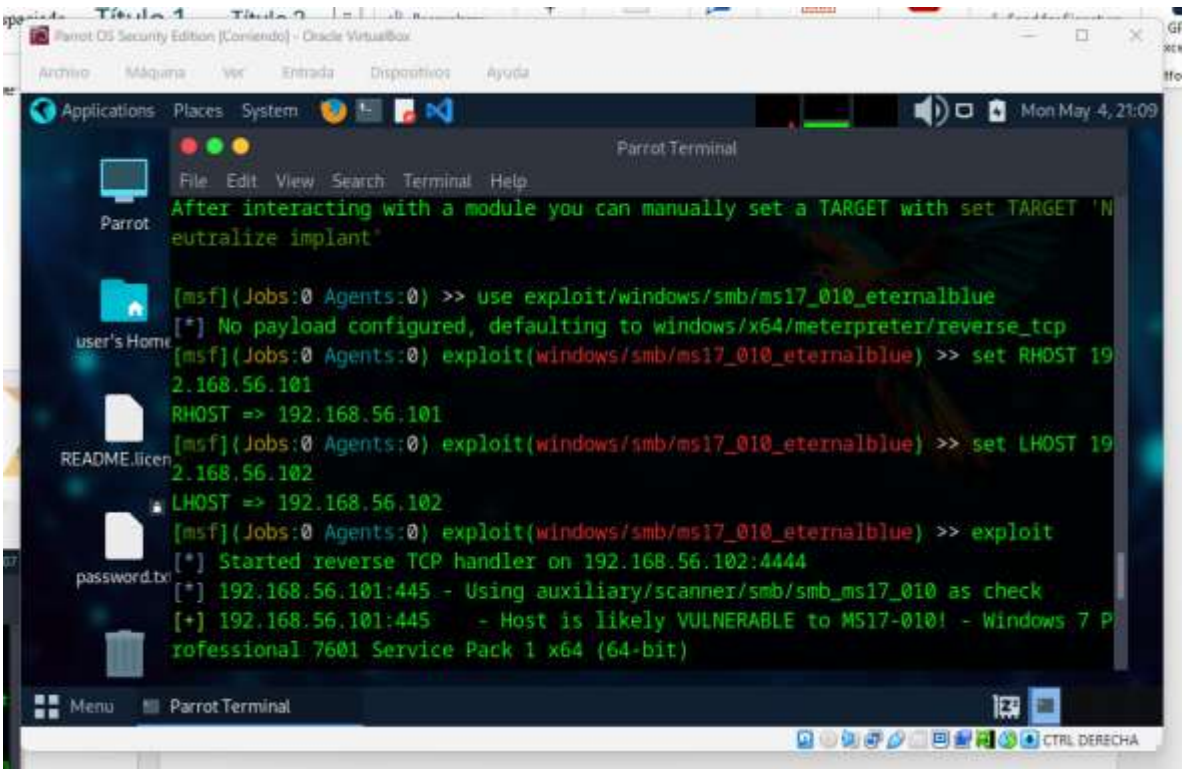
Un aspecto crítico de la arquitectura del ataque: La elección de una Reverse Shell frente a una Bind Shell tradicional se fundamenta en que en una configuración de Bind Shell, el intento de establecer una conexión entrante hacia un puerto abierto en la máquina víctima suele ser

interceptado y bloqueado por las políticas del cortafuegos local. Por el contrario, el uso de una Reverse Shell, delega el inicio de la conexión al propio host comprometido mediante tráfico saliente. Este vector facilita la evasión efectiva de los controles de seguridad perimetrales de la organización.

Al ejecutar la instrucción, la carga maliciosa se transmitió a través del segmento de red y se inyectó en la memoria RAM del servidor.

Figura 4

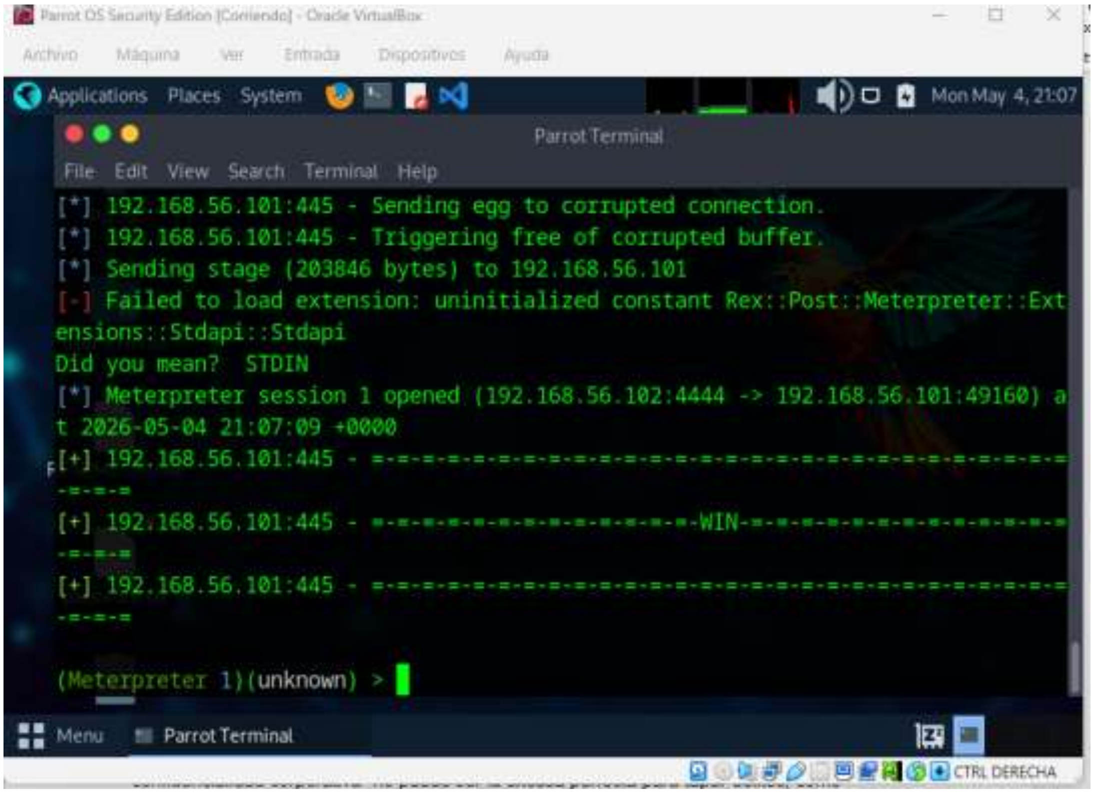
Asignación de IP (Víctima y Host)



Nota. Configuración de los parámetros de red correspondientes al equipo atacante (LHOST) y al equipo víctima (RHOST) en la consola de Metasploit Framework.

Figura 5

Lanzamiento del ataque e inyección del payload



Nota. Proceso de inyección del *payload* en la memoria del servidor víctima tras el lanzamiento y ejecución del *exploit* EternalBlue.

Post-explotación: Solución de problemas y evasión

Durante la ejecución de pruebas de penetración, es habitual identificar discrepancias de arquitectura que exigen procesos de depuración (troubleshooting).

Al ejecutar la carga útil que trae Metasploit por defecto (windows/x64/meterpreter/reverse_tcp), el sistema emitió una confirmación de la sobrescritura exitosa de la memoria (el sistema arrojó el mensaje ETERNALBLUE overwrite completed successfully). Sin embargo, se presentó una incompatibilidad crítica.

Por alguna razón en la arquitectura del Windows de la víctima, la extensión stdapi no se inicializó correctamente, generando una excepción interna. Esto inhabilitó las capacidades avanzadas de Meterpreter para la post-explotación inmediata.

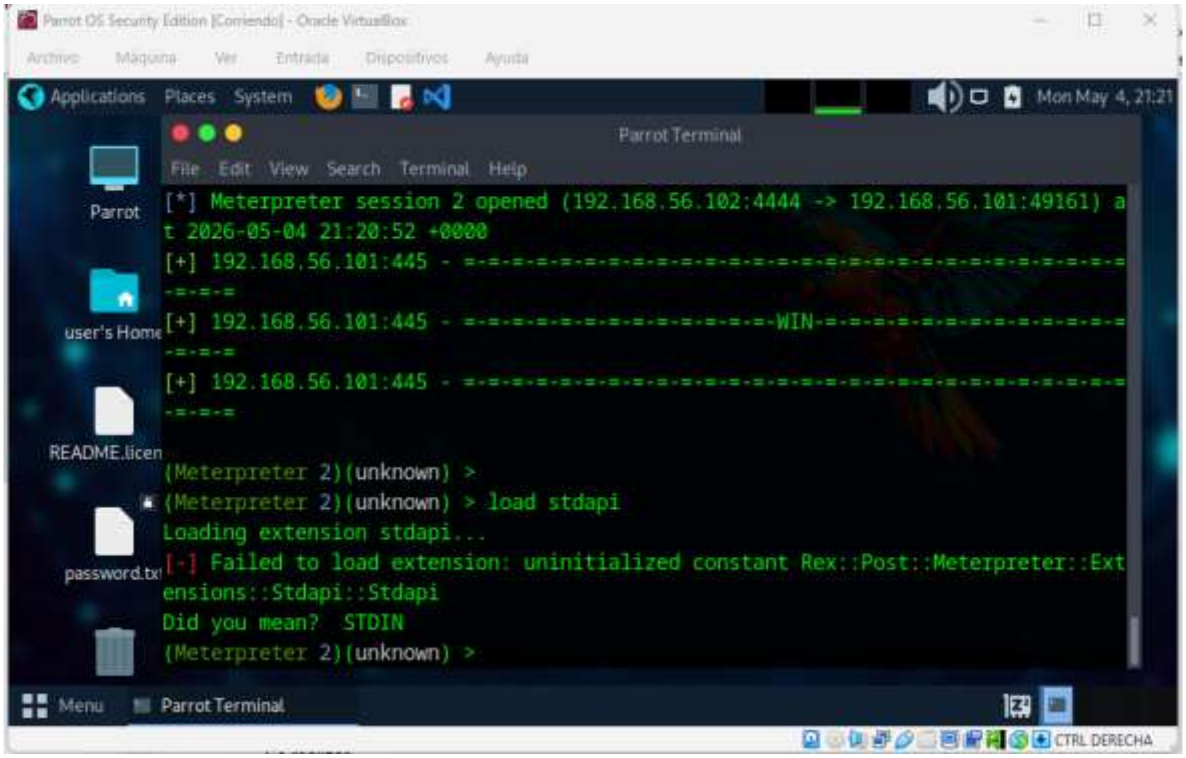
Persistir en la inyección de código inestable sobre la memoria del servidor incrementaba la probabilidad de causar un error de parada del sistema (BSOD), alertando a los mecanismos de defensa organizacionales. Por consiguiente, se modificó la estrategia operativa, degradando la carga útil hacia un shell reverso básico que invoca el intérprete de comandos nativo (windows/x64/shell/reverse_tcp), garantizando estabilidad.

Tras la estabilización del protocolo de transporte SMB, la ejecución subsecuente otorgó acceso directo. El canal de comunicación remota retornó un intérprete de comandos posicionado directamente en el directorio funcional C:\Windows\system32>.

Para confirmar el impacto de la brecha, se ejecutó el comando de enumeración nativa whoami (quién soy). La salida del sistema retornó nt authority\system. Esto valida que el compromiso del sistema operativo fue absoluto y con privilegios de nivel de kernel.

Figura 6

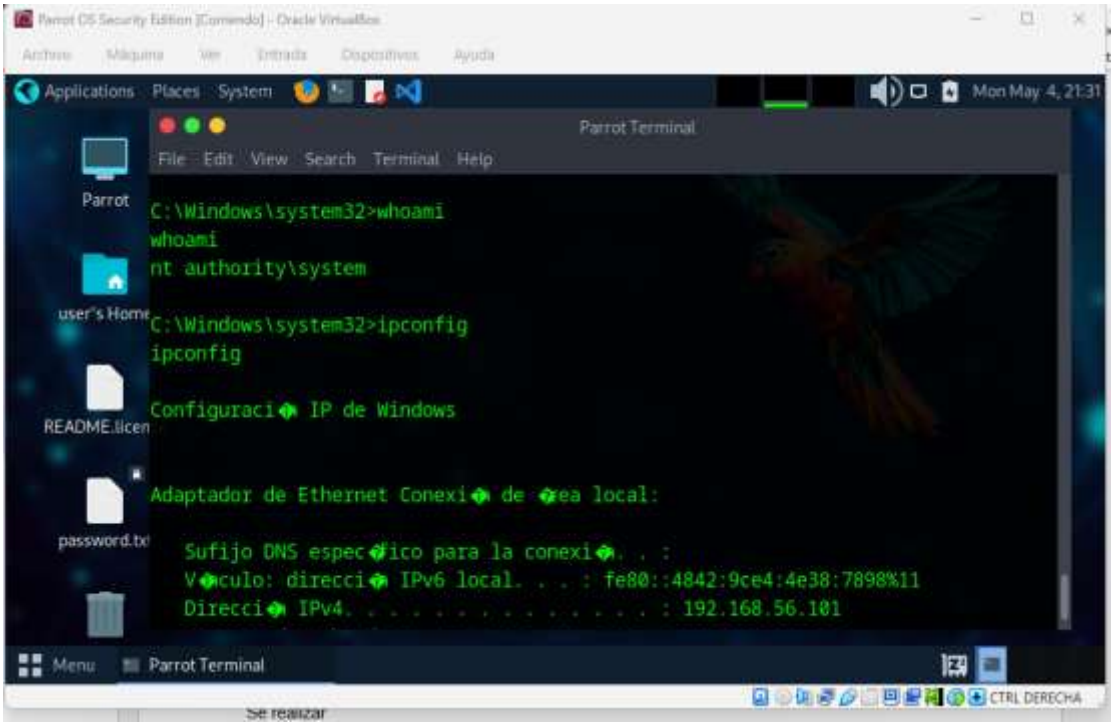
Primer Troubleshooting



Nota. Evidencia del error de compatibilidad presentado durante la carga de la extensión *stdapi* de Meterpreter, lo cual requirió un ajuste táctico en la intrusión.

Figura 7

Acceso exitoso al sistema víctima



Nota. Obtención de una consola interactiva (Reverse Shell) del sistema operativo Windows y confirmación del escalado de privilegios al nivel máximo de administración (*NT AUTHORITY\SYSTEM*).

Movimientos laterales (*Pivoting*) y persistencia

En un ciberataque real, el nodo de compromiso inicial raramente constituye el objetivo estratégico final. Al consolidar el control sobre el Host-A, este se configuró como un nodo de pivotaje técnico. Desde esa consola remota se ejecutó el comando ipconfig para cartografiar los direccionamientos de red internos y descubrir segmentos no expuestos al perímetro exterior.

Para validar la conectividad interna, se transmitieron tramas ICMP (pings) hacia la IP 192.168.56.100 (Host-B). Debido a que el tráfico era confiable, "...el cortafuegos perimetral no interrumpió el tráfico, permitiendo la visibilidad del host secundario. Este procedimiento se define como un movimiento lateral.

La fase de descubrimiento interno identificó que el Host-B ejecutaba el servicio Rejetto HTTP File Server (HFS), corriendo por los puertos web estándar (80 y 8080). Este software representa un riesgo crítico para cualquier empresa. Al ser un servidor de archivos ligero basado en HTTP, constituye un vector ideal para la exfiltración de bases de datos, permitiendo evadir los controles perimetrales al camuflar la carga útil como tráfico web legítimo. Los intentos de cargar un artefacto binario contra este servicio fueron interceptados por las interfaces de protección nativas AMSI y Windows Defender, bloqueando la ejecución en memoria (código de error 0x80004005) debido a la detección de firmas de malware.

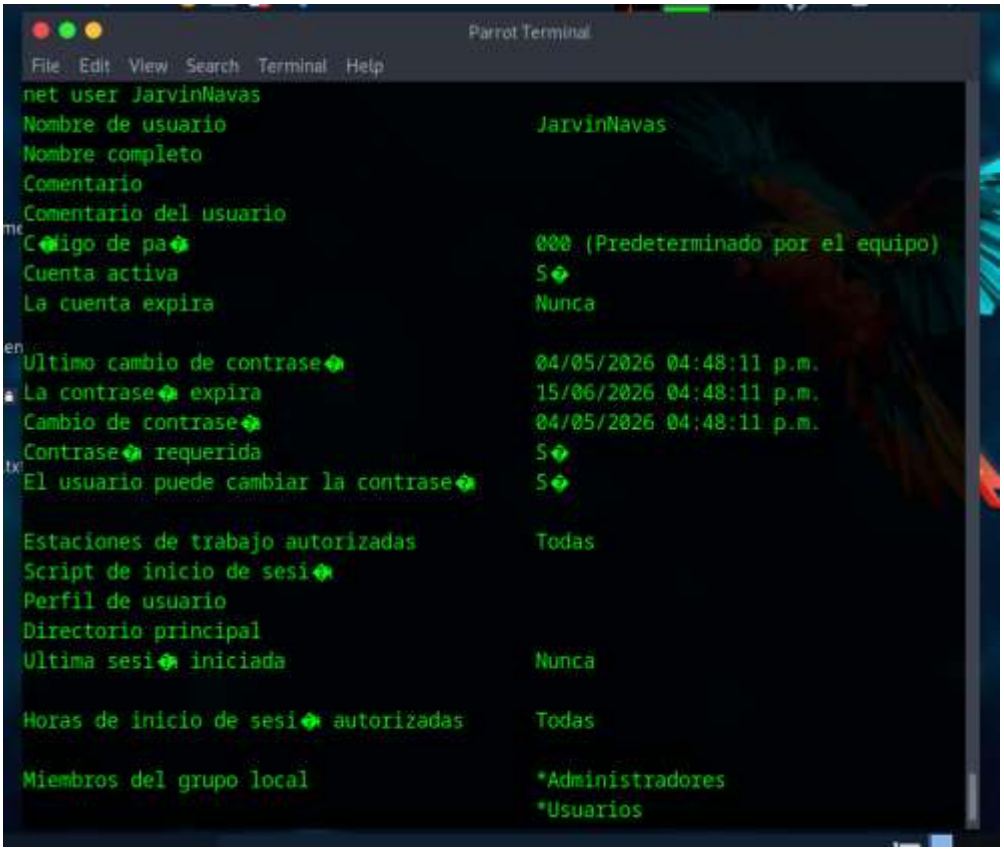
Posteriormente, con el fin de asegurar la persistencia operativa ante eventuales acciones de remediación, se ejecutó una prueba de concepto de persistencia., garantizando el acceso remoto continuo ante eventuales tareas de remediación o reinicios del servidor. Por tal motivo, se procedió al despliegue de una Prueba de Concepto (PoC) de persistencia.

Mediante la línea de comandos, se ejecutó la instrucción net user JarvinNavas Unad2026* /add con el fin de aprovisionar un usuario alterno. Subsiguientemente, se asignaron privilegios administrativos elevados mediante la instrucción net localgroup Administradores JarvinNavas /add. Mediante este comando se garantizó la inclusión de la cuenta comprometida en el grupo de administradores locales.

Si bien este procedimiento genera múltiples eventos a nivel de auditoría (se disparan los Eventos 4720 y 4732 en el visor de Windows), la ausencia de una solución SIEM centralizada impidió la correlación y visibilidad oportuna del compromiso por parte de la organización.

Figura 8

Creación de usuario con total acceso al sistema



Nota. Ejecución de la prueba de concepto de persistencia mediante la creación de un usuario local y su asignación directa al grupo de administradores del sistema.

Mapeo táctico del incidente: Framework MITRE ATT&CK

Con el propósito de estandarizar y correlacionar técnicamente las acciones ofensivas con las capacidades de detección del Blue Team, el ciclo del compromiso se correlacionó con la

matriz del framework global MITRE ATT&CK. Esta matriz es el estándar de la industria para documentar el comportamiento de un atacante.

Tabla 2

Matriz MITRE ATT&CK de la operación ofensiva

Táctica (Objetivo del atacante)	**Técnica Específica (ID MITRE)**	**Acción ejecutada en el entorno de pruebas**
Reconocimiento (TA0043)	Active Scanning (T1595)	Se utilizó arp-scan y Nmap para ver la red y descubrir el puerto SMB expuesto en la 192.168.56.101.
Acceso Inicial (TA0001)	Exploit Public-Facing Application (T1190)	Se ejecutó el exploit de MS17-010 (EternalBlue) contra el puerto 445 sin necesitar contraseñas.
Ejecución (TA0002)	Command and Scripting Interpreter (T1059.003)	Se desplegó la consola nativa de Windows (Command Shell) después del problema que presentamos con Meterpreter.
Escalamiento de Privilegios (TA0004)	Exploitation for Privilege Escalation (T1068)	Al inyectar el código directo en el archivo srv.sys del kernel, el sistema otorgó acceso de NT AUTHORITY\SYSTEM por defecto.
Evasión de Defensas (TA0005)	Indicator Removal / Fileless Threat (T1070)	Se inyectó el ataque directo a la memoria RAM (*Fileless Malware*), esquivando al antivirus ya que nunca tocamos el disco duro.

Descubrimiento (TA0007)	System Network Configuration Discovery (T1016)	Usamos ipconfig desde nuestra consola remota para entender cómo estaba dibujada la topología interna.
Movimiento Lateral (TA0008)	Remote Services / SMB (T1021.002)	Se utilizó el Host-A como nodo de pivote para el envío de peticiones ICMP y descubrir el servicio *Rejetto* corriendo en el Host-B.
Persistencia (TA0003)	Create Account: Local Account (T1136.001)	Se aprovisionó al usuario "JarvinNavas" y se incluyó en el grupo de administradores locales para no perder el acceso a futuro.

(MITRE Corporation, 2024)

Nota. Esta matriz mapea las tácticas y técnicas ofensivas ejecutadas durante el laboratorio práctico, tomando como base el estándar internacional MITRE ATT&CK.

Estrategias de Defensa, Contención y Respuesta a Incidentes (Blue Team).

Frente a un panorama donde cualquier empresa se enfrenta a amenazas avanzadas, la ciberseguridad corporativa no puede limitarse a defensas perimetrales estáticas. Una vez superado el perímetro de seguridad, el enfoque del Blue Team debe centrarse en la contención inmediata del incidente y el aislamiento del vector de amenaza

Metodología de Respuesta a Incidentes (NIST SP 800-61 Rev. 2)

Para garantizar un proceso estructurado y medible, la gestión del incidente se alineó con la Guía de Manejo de Incidentes del NIST SP 800-61 Rev. 2. Esta fase se ejecuta de manera preventiva antes de la materialización de un incidente. Para SecureNova Labs, se establece la Guía de Manejo de Incidentes del Instituto Nacional de Estándares y Tecnología (NIST). La gestión se rigió estrictamente por las cuatro fases de esta metodología: (Cichonski et al., 2012):

1. **Preparación:** Esta etapa se ejecuta de manera preventiva previa a la materialización de un incidente. Para SecureNova Labs, se determinó el establecimiento de una línea base de comportamiento del tráfico y la implementación de soluciones de código abierto orientadas al monitoreo continuo (como Wazuh para registros y Suricata como IPS). El propósito es asegurar que las capacidades de respuesta y los manuales operativos (playbooks) estén disponibles ante un eventual compromiso.
2. **Detección y Análisis (Triaje):** Consiste en la validación técnica del compromiso y la evaluación de su criticidad. A través del análisis de telemetría y conexiones activas en tiempo real (netstat y TCPView), se identificó tráfico anómalo en el puerto 445/TCP y sesiones salientes no autorizadas (Reverse Shells) hacia los puertos 4444/TCP y 8080/TCP.
3. **Contención, Erradicación y Recuperación:**
    - **Erradicación:** Comprende la finalización forzada de los hilos de ejecución asociados al framework de explotación. Asimismo, se eliminaron los mecanismos de persistencia mediante la supresión de la cuenta local no autorizada y se aplicó la actualización correspondiente para mitigar de raíz la vulnerabilidad de SMBv1.

- **Contención:** La acción inicial consistió en ejecutar el aislamiento lógico del nodo comprometido (Host-A). Se mantuvo el estado de encendido del activo bajo el principio forense de preservación de evidencia volátil contenida en la memoria RAM.
- **Recuperación:** Consiste en el retorno paulatino y controlado del activo a la red de producción, manteniéndolo bajo monitoreo estricto para detectar intentos latentes de conexión hacia servidores de Comando y Control (C2)

4. **Actividades Post-Incidente (Lecciones aprendidas):** Es el cierre del ciclo, y se materializa en la elaboración del informe técnico de lecciones aprendidas. En esta fase se formalizan las brechas identificadas, la cadena de custodia y se estructuran los controles definitivos de mitigación como aplicar las políticas de configuración segura (Center for Internet Security [CIS], 2024).

Playbook táctico de respuesta ante intrusiones (RCE)

La adopción de marcos metodológicos requiere ser operacionalizada mediante guías de ejecución rápida ante situaciones de contingencia. Por ello, se estructuró un playbook alineado con los criterios del NIST para estandarizar los flujos de trabajo del CSIRT ante compromisos en el servicio SMB.

Tabla 3

Playbook CSIRT: Contención de ataques RCE y movimientos laterales

Fase (NIST)	Acción de respuesta	Herramienta técnica	Responsable asignado

Detección	Identificar conexiones ESTABLISHED en puertos no estándar o picos de tráfico en SMB.	SIEM (Wazuh), netstat, TCPView	Analista SOC (Nivel 1)
Detección	Aislar procesos sospechosos derivados de procesos legítimos de Windows (ej. un *cmd.exe* debajo de *spoolsv.exe*).	Process Explorer	Analista Forense (Nivel 2)
Contención	Deshabilitar el puerto o reasignar a una VLAN aislada	Consola del Switch / VirtualBox	Ingeniero de Redes
Contención	Bloqueo de las IPs del atacante directamente en la lista negra del perímetro.	Suricata IPS / Firewall	Ingeniero de Seguridad
Erradicación	Extraer una imagen forense exacta (volcado) de la memoria RAM antes de manipular el equipo	FTK Imager / DumpIt	Perito Informático
Erradicación	Analizar ese volcado para sacar el *payload* y buscar claves o credenciales robadas.	Volatility Framework	Malware Analyst

Recuperación	Finalizar procesos maliciosos, borrar cuentas ocultas y aplicar el parche MS17-010.	PowerShell / WSUS	SysAdmin
Post-Incidente	Actualizar las reglas del IPS y del SIEM con los indicadores de compromiso extraídos de la memoria RAM.	Plataformas MISP	Analista Blue Team

Nota. El presente playbook describe las acciones secuenciales, las herramientas recomendadas y los responsables técnicos para la correcta contención y erradicación del incidente.

Detección temprana y triaje del incidente

Ante la generación de una alerta crítica de red, la prioridad operativa del Blue Team consiste en evitar la propagación de la amenaza. Este procedimiento se denomina determinación del alcance del compromiso. La estructuración de estas fases defensivas se apoyó adicionalmente en los lineamientos de gestión de incidentes y ciberseguridad propuestos por las instituciones académicas nacionales (CSIRT Académico UNAD, 2024; Universidad de Cundinamarca, 2021; Universidad EAN, 2021; Zambrano Hernández & Cárdenas Corral, 2024).

El diagnóstico preciso del vector de acceso inicial y los mecanismos de persistencia requiere la inspección sistemática de los procesos y llamadas del sistema en el kernel de Windows. El uso de herramientas de monitoreo como TCPView o comandos nativos netstat -ano resulta fundamental para el diagnóstico. Los analistas deben enfocar la inspección en procesos legítimos que muestren un comportamiento anómalo, como la apertura no justificada de sockets de red.

En el Host-A, este procedimiento evidenció conexiones TCP en estado ESTABLISHED hacia hosts externos mediante los puertos 4444/TCP y 8080/TCP. Estas conexiones representan un indicador de compromiso inequívoco de la ejecución de una Reverse Shell activa bajo el control de un actor externo

Contención y preservación de evidencia volátil

Tras la confirmación técnica del compromiso, se inicializó la fase de contención. El mecanismo inmediato consistió en el aislamiento lógico del host afectado. En entornos de producción, este control se asocia a la reasignación de puertos a una VLAN de cuarentena; en el laboratorio virtual, se inhabilitó la interfaz de red corporativa. Al hacer esto en la Capa 2, se neutraliza el vector de ataque y se protege de manera inmediata la integridad del resto de los servidores.

De acuerdo con los principios de la informática forense (basada en la norma RFC 3227): **el orden de recolección de evidencia digital es un factor crítico.**. Por ende, se prohíbe el reinicio o apagado del activo comprometido

Como el ataque *EternalBlue* funciona como *Fileless Malware* (no deja archivos en el disco duro, todo lo hace en la RAM), un reinicio prematuro del sistema operativo purgaría los datos volátiles destruyendo la evidencia forense residente en memoria. Esto causaría la pérdida irreversible de los hilos de proceso inyectados y los registros de conexión IP del atacante. La preservación del estado activo del host garantiza las condiciones óptimas para la adquisición del volcado forense.

Adquisición y Análisis de la Memoria RAM

La investigación detallada del incidente requiere la ejecución de un análisis forense de memoria RAM.

- **Fase de Adquisición:** Con el Host-A ya aislado pero encendido, el especialista forense extrae una imagen bit a bit de la memoria RAM. Para mitigar la alteración de los datos, se emplearon herramientas estandarizadas como FTK Imager ejecutadas desde medios de almacenamiento externos. Este procedimiento genera una imagen forense (.raw o .mem) que preserva el estado exacto del sistema en ejecución.
- **Fase de Análisis:** El volcado de memoria fue exportado a una estación forense aislada para su análisis mediante *Volatility Framework*. En la investigación se ejecutaron los siguientes módulos (plugins) de análisis
    - netscan: Despliega las conexiones de red activas en el momento de la adquisición de la memoria. Se identificó el socket reverso establecido hacia la IP del atacante (192.168.56.102:4444).
    - pslist y pstree: En este segmento de memoria se identificó el código binario inyectado por Metasploit. Permiten detectar anomalías como la ejecución de un intérprete de comandos (cmd.exe) derivado de un proceso de sistema legítimo (spoolsv.exe). Mediante este comando se localizó el código binario inyectado por el framework ofensivo.
    - malfind: Es el plugin forense más relevante. Este comando busca partes de la memoria RAM que tienen permisos anómalos de Ejecución, Lectura y Escritura, los cuales no se encuentran vinculados a ningún archivo legítimo del sistema de almacenamiento. En este segmento de memoria se localizó el código binario inyectado por Metasploit.

Implementación de herramientas de monitoreo y contención (SIEM e IPS)

Con el fin de migrar hacia una postura defensiva automatizada, SecureNova Labs requiere centralizar la visibilidad de los eventos de seguridad. Debido a las restricciones presupuestarias de la organización, se diseñó una arquitectura defensiva basada en soluciones de código abierto de nivel empresarial.

- **Wazuh (XDR y SIEM):** Desplegado mediante un agente de recolección en el Host-A. Proporciona análisis de comportamiento y detección de amenazas en tiempo real. Se establecieron reglas para generar alertas ante eventos como:
    - **Fuerza bruta para moverse por la red:** Correlación de múltiples fallos de autenticación (ID de evento 4625) seguidos de un acceso exitoso (ID de evento 4624) en un intervalo reducido de tiempo. Ejecución de scripts ofuscados: Detección de instancias de PowerShell con argumentos de evasión, tales como -WindowStyle Hidden o -ExecutionPolicy bypass, característicos de vectores de compromiso inicial.
    - **Comandos maliciosos escondidos:** Detección de la ejecución de instancias de PowerShell con parámetros de ofuscación o evasión (-WindowStyle Hidden) o para evadir las restricciones (-ExecutionPolicy bypass), comportamiento típicamente asociado a malware basado en macros.
    - **Respuesta Activa:** Configuración de módulos automáticos orientados al bloqueo inmediato de la dirección IP de origen en el cortafuegos local o la terminación forzada del subproceso malicioso de forma automatizada. Suricata (NIDS/NIPS en modo Inline): Configurado como control perimetral primario de contención.

- **Suricata (NIDS/NIPS en modo *Inline*):** "Este componente constituye la barrera primaria de contención. Opera en modo prevención (IPS) ejecutando inspección profunda de paquetes en la capa de aplicación. Ante la identificación de tramas malformadas asociadas a EternalBlue, el sistema ejecuta acciones de descarte (drop) antes de que afecten al host de destino.
- **Firewall de Windows Avanzado:** La implementación de directivas restrictivas de entrada y salida actúa como control complementario sin costo de licenciamiento. La efectividad de las soluciones tecnológicas de monitoreo depende directamente del aprovisionamiento de firmas y reglas específicas de detección.

Análisis técnico de las reglas de detección

El despliegue de estas soluciones tecnológicas requiere la configuración de firmas y reglas específicas para su correcto funcionamiento. A continuación, se detalla la configuración de las reglas de detección implementadas en el entorno de pruebas:

Regla de prevención en Suricata (Firma para bloquear EternalBlue): Implementación de una firma orientada a la detección y mitigación del tráfico anómalo en el protocolo SMB. Análisis de la firma: El sistema analiza el flujo entrante dirigido al puerto 445/TCP del segmento local ($HOME_NET). Si la carga útil coincide con el patrón hexadecimal característico del exploit, la trama es descartada inmediatamente, neutralizando la fase de entrega.

YAML

drop smb any any -> $HOME_NET 445 (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:to_client,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; classtype:attempted-admin; sid:2024218; rev:2;)

Regla de detección en Wazuh (Creación de usuarios ocultos): Configuración del archivo local_rules.xml para supervisar la generación del ID de evento 4720 de Windows, clasificándolo como una alerta de alta severidad vinculada a técnicas de persistencia.

XML

```
<rule id="100001" level="12">
 <if_sid>60103</if_sid>
 <field name="win.system.eventID">^4720$</field>
 <description>Alerta Crítica: Creación de cuenta de usuario local no programada. Posible persistencia.</description>
 <mitre>
  <id>T1136.001</id>
 </mitre>
</rule>
```

Aseguramiento de la infraestructura (*Hardening*)

La remediación de los efectos del ataque carece de valor permanente si persisten las vulnerabilidades subyacentes en la infraestructura. Para mitigar de raíz los vectores expuestos, se requiere la aplicación obligatoria de controles de endurecimiento (hardening):

- **Inhabilitación definitiva de protocolos obsoletos:** El protocolo SMBv1, agente facilitador del vector de explotación, carece de controles criptográficos modernos. Es

mandatoria su inhabilitación a través de Directivas de Grupo (GPO) y obligar a todos los equipos a usar SMBv3.

- **Ciclo de parches estricto:** La simulación de intrusión evidenció deficiencias significativas en las prácticas de administración tecnológica. Es imperativa la creación de una política que garantice la instalación de actualizaciones críticas de seguridad en los servidores en menos de 48 horas.
- **Principio de Mínimo Privilegio:** Se identificó que las cuentas de usuario estándar poseían privilegios excesivos en el sistema. Se deben remover los accesos al grupo de administradores locales y desplegar soluciones como Microsoft LAPS para la rotación automatizada de credenciales locales, mitigando vectores de movimiento lateral basados en Pass-the-Hash.
- **Control de aplicaciones (AppLocker):** Implementación de directivas mediante Windows Defender Application Control.

Diferencias operativas: Blue Team vs. CSIRT

Para cerrar este informe y mejorar la gobernanza en SecureNova Labs, es fundamental que la gerencia diferencie los alcances preventivos de los reactivos, garantizando la separación funcional de los equipos de seguridad

- **El Blue Team** ejerce funciones operativas continúas orientadas a la prevención, configuración segura y monitoreo. Sus tareas principales abarcan el análisis de telemetría, la optimización del SIEM, la ejecución de Threat Hunting y el ajuste de políticas de acceso.
- **El CSIRT (Equipo de Respuesta a Incidentes)**, en cambio actúa como la unidad de respuesta operativa, operando bajo un enfoque estrictamente reactivo. Son totalmente

reactivos. Su activación se produce tras la confirmación de una brecha de seguridad que supera los controles preventivos primarios de la organización corporativa. Su objetivo primordial consiste en mitigar el impacto del incidente... y restablecer la continuidad del negocio en el menor tiempo posible.

Conclusiones y Recomendaciones

Propuesta de política corporativa: Gestión de parches y vulnerabilidades

El análisis técnico de la simulación de intrusión evidenció que el compromiso del sistema mediante la vulnerabilidad MS17-010 (EternalBlue) no fue el resultado de un ataque altamente sofisticado, sino la consecuencia de deficiencias críticas en la higiene tecnológica de la organización. Se establece que la implementación de defensas técnicas carece de efectividad si no está respaldada por directrices administrativas de cumplimiento obligatorio. Por consiguiente, se propone a la alta gerencia de SecureNova Labs la adopción y puesta en marcha de una política formal para la gestión de parches y vulnerabilidades.

El objetivo central de esta política es proteger los activos de información y la infraestructura de servidores de la organización mediante la estructuración de un ciclo continuo

de identificación de fallos, evaluación de parches en entornos controlados (sandboxing) y su respectiva implementación oportuna. Con esto, se busca reducir drásticamente el riesgo de exposición a ataques de ejecución remota de código (RCE) y evitar los movimientos laterales. En cuanto a su alcance, esta normativa se debe aplicar de manera irrestricta sobre la totalidad de los componentes tecnológicos de la empresa, abarcando sistemas operativos Windows y Linux, dispositivos de red, aplicaciones de terceros y bases de datos, independientemente de su ubicación física o de su despliegue en la nube.

Para garantizar la ejecución de la política, se definen roles y responsabilidades específicos en tres niveles. El Oficial de Seguridad de la Información (CISO) funge como el responsable máximo, encargado de aprobar la directriz, auditar su cumplimiento y autorizar de forma excepcional la aceptación de riesgos en escenarios donde la aplicación de un parche afecte un sistema crítico y requiera una solución temporal. Por su parte, el equipo Blue Team o CSIRT asume la responsabilidad de realizar la vigilancia continua de nuevas vulnerabilidades (CVE) y de ejecutar escaneos periódicos mediante herramientas especializadas. Finalmente, los administradores de TI tienen a su cargo la fase operativa, la cual incluye la descarga, la validación en servidores de prueba y el despliegue masivo de las actualizaciones mediante sistemas centralizados.

Para asegurar la oportunidad en la mitigación de riesgos, la política establece Acuerdos de Nivel de Servicio (SLA) estrictos para la aplicación de parches, fundamentados en la severidad de la falla según el estándar internacional CVSS. Las vulnerabilidades críticas (CVSS 9.0 a 10.0), que permiten compromisos severos sin autenticación previa y facilitan ataques de secuestro de datos, exigen una mitigación en un plazo máximo de 24 a 48 horas. Para las vulnerabilidades altas (CVSS 7.0 a 8.9), cuyo éxito depende de la interacción del usuario o de la

posesión de credenciales, se establece un límite de siete días. Las fallas de severidad media (CVSS 4.0 a 6.9) deben ser abordadas dentro de la ventana de mantenimiento mensual con un margen de 15 días. Por último, las vulnerabilidades bajas (CVSS 0.1 a 3.9) pueden ser consolidadas y remediadas en ciclos trimestrales de 30 a 60 días, considerando su reducida probabilidad de explotación en entornos de producción.

Conclusiones

El desarrollo de este seminario especializado permitió establecer que la ejecución de actividades técnicas ofensivas y defensivas en ciberseguridad carece de validez y expone al profesional a graves consecuencias legales si no se enmarca en la normativa vigente. Se evidenció que la aceptación de acuerdos de confidencialidad que induzcan a la omisión de denuncia o al encubrimiento de delitos, como el ciber espionaje, contraviene de forma directa la Ley 1273 de 2009 y los lineamientos del Código de Ética del Consejo Profesional Nacional de Ingeniería (COPNIA). Por consiguiente, el rigor ético y normativo constituye el eje transversal ineludible de cualquier auditoría de sistemas en el entorno corporativo.

Por otra parte, la simulación de intrusión demostró empíricamente el alto impacto que genera la persistencia de protocolos obsoletos en la infraestructura corporativa. La explotación exitosa de la vulnerabilidad MS17-010 (EternalBlue) confirmó que mantener servicios

heredados, como el SMBv1, representa un fallo arquitectónico crítico. Esta brecha facilitó la corrupción de la memoria del servidor y permitió la obtención del nivel máximo de privilegios en el sistema sin requerir ningún tipo de autenticación o interacción previa.

Asimismo, los resultados del entorno de pruebas ratificaron los riesgos inherentes a las arquitecturas de red planas. Se verificó que el compromiso inicial de un equipo fronterizo no constituye el objetivo final de un atacante, sino el vector de entrada para ejecutar movimientos laterales de manera sigilosa. La ausencia de segmentación interna en la red evaluada facilitó la visibilidad y el acceso irrestricto hacia otros servidores críticos, demostrando que, una vez vulnerado el perímetro exterior, la seguridad global de la empresa colapsa si no existen barreras de contención secundarias.

Finalmente, el ejercicio defensivo comprobó la eficacia operativa de las herramientas de código abierto para la consolidación de un entorno corporativo seguro. La configuración e integración de soluciones libres de licenciamiento, tales como Wazuh y Suricata, permitió estructurar un mecanismo sólido para la detección de ataques, el monitoreo profundo del tráfico y la mitigación de amenazas en tiempo real. Esto demuestra que es completamente viable establecer una postura defensiva madura y de nivel empresarial optimizando el presupuesto mediante la implementación de estándares metodológicos rigurosos.

Recomendaciones

A partir de los hallazgos documentados, se recomienda a la gerencia de la organización adoptar de manera rigurosa los controles de seguridad establecidos por el Center for Internet Security (CIS). Esto implica abandonar las configuraciones predeterminadas de los sistemas, deshabilitar definitivamente protocolos obsoletos en todos los segmentos e implementar políticas de cifrado estandarizadas. En paralelo, resulta perentorio transitar hacia una arquitectura de Confianza Cero o Zero Trust (Rose et al., 2020), asumiendo la premisa de que las amenazas pueden originarse o residir internamente. Esta transición requiere la obligatoriedad de la autenticación de doble factor (MFA) para los accesos administrativos y la revocación general de privilegios de administrador local a los usuarios estándar.

Para materializar estas medidas sin afectar la operatividad del negocio, se sugiere ejecutar un plan de trabajo estructurado en tres horizontes temporales de implementación. En el corto plazo, los esfuerzos deben centrarse en asegurar las identidades y los puntos finales mediante un inventario exhaustivo de la red, la actualización imperativa hacia el protocolo SMBv3 y el

despliegue de soluciones de detección avanzadas (EDR) que permitan bloquear ejecuciones anómalas directamente en la memoria de los equipos.

A mediano plazo, la prioridad técnica debe enfocarse en la segmentación estricta de la infraestructura tecnológica. Es imperativo abandonar la topología de red plana para aislar lógicamente las bases de datos, los repositorios de archivos y las estaciones de trabajo en redes de área local virtuales (VLAN) totalmente independientes. Esta labor debe complementarse con la reconfiguración de los cortafuegos internos bajo una política de denegación por defecto (Default Deny), garantizando que el compromiso individual de una máquina no comprometa los segmentos adyacentes.

A largo plazo, se recomienda automatizar los procesos de defensa correlacionando los registros del sistema SIEM implementado con las capacidades de respuesta perimetral, con el objetivo de habilitar bloqueos automáticos ante alertas de criticidad alta. Para garantizar una mejora continua, la organización debe programar escaneos automáticos de vulnerabilidades con una periodicidad semanal y establecer ejercicios de entrenamiento cruzado (Purple Teaming). Estas simulaciones periódicas, donde interactúen estrategias ofensivas y defensivas, permitirán validar de forma constante la efectividad de los controles instalados y afinar la capacidad de respuesta ante incidentes cibernéticos reales.

Evidencias de Sustentación

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

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

Referencias Bibliográficas

Angarita Carrascal, J. A. (2021). *Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team*. Repositorio Institucional UNAD. https://repository.unad.edu.co/jspui/bitstream/10596/54756/1/jaangaritac.pdf

Center for Internet Security [CIS]. (2024). *CIS Benchmarks*. https://www.cisecurity.org/cis-benchmarks/

Centro de Respuestas a Incidentes Informáticos [CSIRT Académico UNAD]. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS*. Universidad Nacional Abierta y a Distancia. https://csirt.unad.edu.co/images/2023/Publicaciones/13102023_OK_-_Guia_para_la_valoraci%C3%B3n_y_evaluaci%C3%B3n_de_riesgos_de_ciberseguridad_de_los_activos_de_informaci%C3%B3n_final.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Congreso de la República de Colombia. (2009, 5 de enero). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se dictan otras disposiciones.

SUIN-Juriscol. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699

Congreso de la República de Colombia. (2012, 17 de octubre). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. SUIN-Juriscol. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

Consejo Profesional Nacional de Ingeniería [COPNIA]. (2015). *Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares*. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Dominguez Sierra, R. O. (2020). Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team. Repositorio Institucional UNAD. https://repository.unad.edu.co/jspui/bitstream/10596/37164/1/1069724846.pdf

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

Instituto Nacional de Ciberseguridad [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-tussistemas

Instituto Nacional de Ciberseguridad [INCIBE]. (2021). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Lockheed Martin Corporation. (2015). *The Cyber Kill Chain®. Defending Against Advanced Persistent Threats*. Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Medina Beltran, P. E. (2023). *Capacidades técnicas, legales y de gestión para equipos blue team y red team*. Repositorio Institucional UNAD. https://repository.unad.edu.co/jspui/bitstream/10596/65364/1/pemedinab.pdf

Microsoft. (2017). *Boletín de seguridad de Microsoft MS17-010 - Crítico: Actualización de seguridad para Microsoft Windows SMB Server (4013389)*. Microsoft Learn. https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

MITRE Corporation. (2024). *MITRE ATT&CK® Framework*. The MITRE Corporation. https://attack.mitre.org/

Presidencia de la República de Colombia. (2013, 27 de junio). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. SUIN-Juriscol. https://www.suin-juriscol.gov.co/viewDocument.asp?id=1276081

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sello Editorial UNAD. (2024). Una Mirada a Metodologías Para Pruebas de Penetración en Ciberseguridad. Boletín de Ciberseguridad Institucional. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

Universidad de Cundinamarca. (2021). *Gestión de Incidentes de Seguridad de la Información (ESG-SSI-P09).* Sistema de Gestión de la Calidad.

https://www.ucundinamarca.edu.co/sgsi/wp-content/uploads/2021/07/ESG-SSI-P09_V1.pdf

Universidad EAN. (2021). *Ciberseguridad: Escuela de verano*. Repositorio Institucional EAN. https://universidadean.edu.co/sites/default/files/Escuela_de_verano/2021/Ciberseguridad/Ciberseguridad.pdf

Zambrano Hernández, H. J., & Cárdenas Corral, H. 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, A. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad OSSTMM, aplicado a la rama judicial, seccional Armenia* [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/17410

Apéndice A: Reporte Similitud Turnitin

Figura 9

Reporte Similitud Turnitin

Nota. Reporte de originalidad generado por la plataforma Turnitin, el cual evidencia el índice de similitud del documento final.

Apéndice B: Bitácora de explotación, escalada de privilegios y movimiento lateral

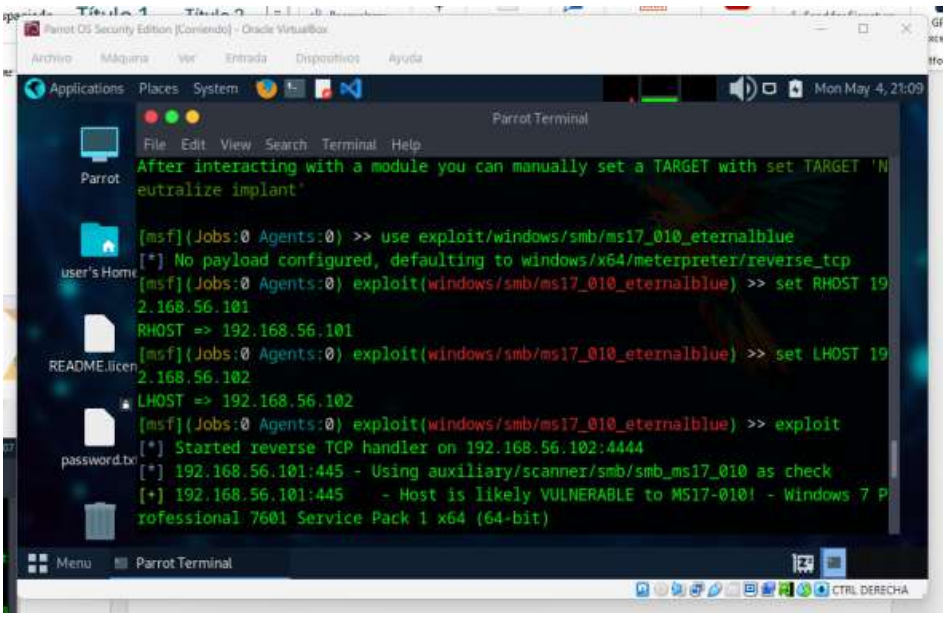
En este anexo dejamos el registro exacto de los comandos y respuestas que se presentaron al interactuar con la consola de Metasploit Framework.

El objetivo de esta bitácora es mostrar la evidencia real del paso a paso del ataque: desde la configuración inicial del exploit EternalBlue y apuntamos a la máquina víctima, pasando por el error de compatibilidad generado por la librería avanzada de Meterpreter (stdapi), y la remediación aplicada inyectando una *Reverse Shell* básica y nativa de Windows. Finalmente, se anexan las capturas donde el propio sistema confirma que se obtuvo el nivel máximo de permisos (NT AUTHORITY\SYSTEM).

1. Configuración del exploit EternalBlue en msfconsole (RHOST y LHOST)

Figura 10

Configuración Exploit

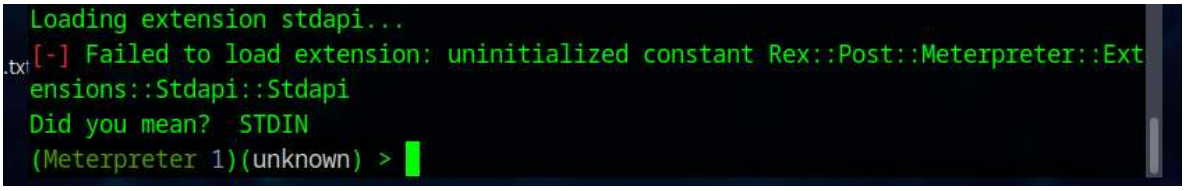


Nota. Detalle de la selección y parametrización del módulo específico de explotación para la vulnerabilidad MS17-010 dentro del entorno de Metasploit.

2. Intento inicial con Meterpreter y error de carga en la sesión (stdapi)

Figura 11

Meterpreter failed

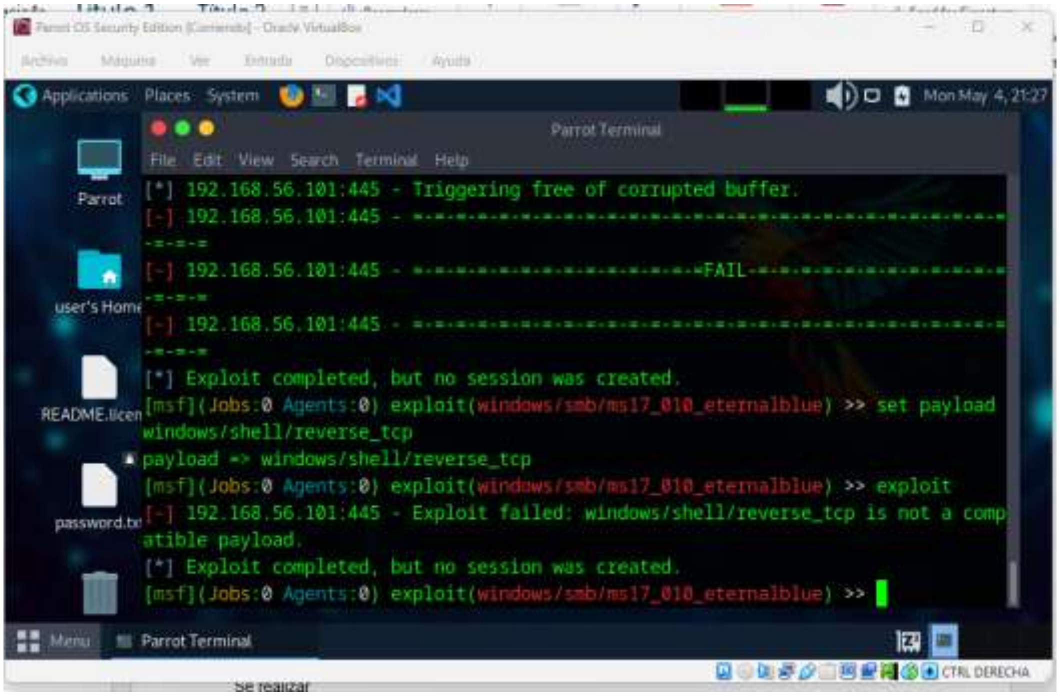


Nota. Vista en detalle del fallo de inicialización de la sesión avanzada de Meterpreter tras la sobrescritura de la memoria del servidor.

3. Degradación controlada del ataque y cambio a payload de Shell básica

Figura 12

Degradación payload

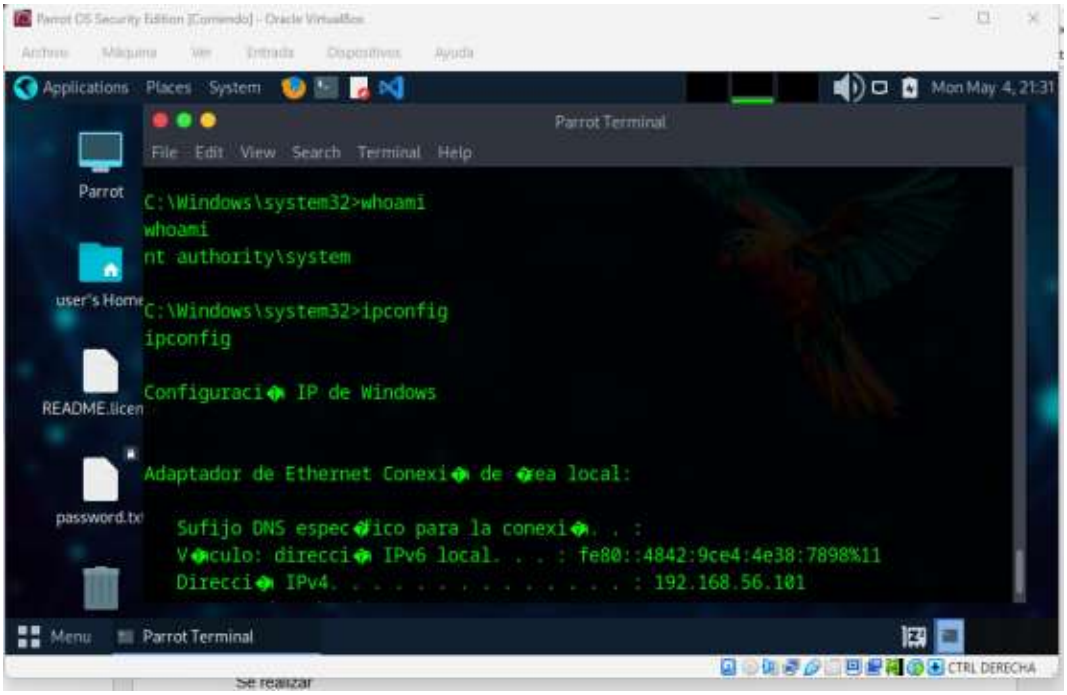


Nota. Degradación controlada del ataque mediante la asignación de un *payload* de conexión inversa rudimentario (windows/shell/reverse_tcp) para estabilizar el acceso al servidor.

4. Consola de sistema (cmd.exe) obtenida y verificación de privilegios máximos (whoami)

Figura 13

Verificación de Privilegios



Nota. Ejecución de comandos de reconocimiento nativos (whoami e ipconfig) desde la sesión remota para verificar el control administrativo y analizar la topología de red subyacente.

Apéndice C: Acuerdo De Reglas De Enfrentamiento (Roe) Para Pruebas De Penetración

1. Objetivo y alcance de la autorización Mediante este documento, SecureNova Labs (en adelante "El Cliente") le da permiso expreso al Equipo Auditor (*Red Team*) para realizar ataques informáticos controlados contra el segmento de red 192.168.56.0/24. Este permiso se otorga con el único propósito de encontrar fallas de seguridad. Al dejar este consentimiento firmado y por escrito, se blinda legalmente la operación y se evita incurrir en el delito de "acceso abusivo a un sistema informático" que castiga el Artículo 269A de la ley colombiana.

2. Metodologías permitidas y restringidas El equipo cuenta con autorización explícita para el uso de herramientas de escaneo de puertos (como Nmap), buscar vulnerabilidades y utilizar entornos de explotación (como Metasploit Framework). Sin embargo, queda totalmente prohibido lanzar ataques de Denegación de Servicio (DDoS) o utilizar técnicas que afecten la disponibilidad del negocio.

3. Manejo de evidencia y privacidad de datos (Ley 1581 de 2012) Si el *Red Team* logra vulnerar un servidor que almacene bases de datos, los auditores tienen estrictamente prohibido copiar, descargar, extraer o siquiera visualizar registros que contengan información personal de usuarios o clientes (PII). Para demostrar que el ataque fue un éxito (Prueba de Concepto), el equipo solo podrá inyectar un archivo de texto inofensivo o correr un comando nativo (como whoami) para evidenciar el nivel de privilegios obtenidos en la máquina objetivo.

4. Deber de denuncia y cláusula de indemnidad Si durante el transcurso de la prueba el Equipo Auditor identifica evidencia de delitos reales que ya estaban ahí (por ejemplo, redes de espionaje de terceros o material de abuso infantil), el ataque simulado se suspenderá en ese mismo instante. El equipo procederá a aislar el servidor para proteger la memoria RAM y cuidar la cadena de custodia, notificando de inmediato a las autoridades competentes. Esta cláusula es innegociable, en estricto cumplimiento del deber de denuncia ciudadana y la ética profesional que exige el COPNIA.