Capacidades técnicas, legales y de gestión para equipos blue team y red team

Alonso Dueñas Vaca

Asesor

Ingeniero Luis Fernando Zambrano Hernández

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Sociales Artes y Humanidades ECSAH

Programa

2025

Esta página opcional

_____

Nombre Director de Trabajo de Grado

_____ _____

Jurado Jurado

2025

Agradecimientos

Quiero expresar mi sincero agradecimiento a los tutores de la Universidad Nacional Abierta y a Distancia (UNAD) por su acompañamiento constante y su dedicación en la transmisión de conocimientos. De igual manera, agradezco a la UNAD por brindar un entorno académico que facilitó el desarrollo de nuevas habilidades fundamentales, no solo para el ejercicio profesional, sino también para la vida personal. Este apoyo ha sido clave para fortalecer mi formación y enfrentar con mayor seguridad los retos del campo de la ciberseguridad.

Resumen

El presente informe técnico, documenta un ejercicio práctico de ciberseguridad en un entorno controlado basado en la empresa ficticia CyberFort Technologies. El objetivo principal fue analizar la vulnerabilidad MS17-010, conocida como EternalBlue, en el protocolo SMBv1 de sistemas Windows, mediante pruebas de intrusión tipo Red Team, y desarrollar estrategias de contención desde el enfoque Blue Team. Para ello, se emplearon herramientas especializadas como Nmap para el escaneo de puertos y detección de vulnerabilidades, así como Metasploit Framework para la explotación remota de la falla, lo que permitió obtener acceso privilegiado al sistema y evidenciar riesgos críticos de control total por parte del atacante.

El informe resalta la importancia de identificar vulnerabilidades mediante técnicas de penetración para fortalecer la seguridad informática, evitando así posibles brechas que comprometan la confidencialidad, integridad y disponibilidad de los activos digitales. La fase de defensa incluyó acciones inmediatas de aislamiento del sistema comprometido, eliminación de cuentas maliciosas y propuestas de hardenización, como la desactivación del protocolo vulnerable, aplicación de parches y restricción de puertos, complementadas con el monitoreo mediante herramientas SIEM y sistemas de detección de intrusiones.

Finalmente, el estudio enfatiza el valor formativo y diagnóstico del ejercicio para el desarrollo de competencias técnicas en seguridad ofensiva y defensiva, aportando a la madurez organizacional y la capacidad de respuesta ante amenazas reales. La integración de hallazgos, medidas forenses y recomendaciones contribuye a fortalecer la postura de seguridad y la resiliencia de las infraestructuras digitales en contextos corporativos actuales.

Palabras clave: Ciberseguridad, Intrusión, Mitigación, Red Team, Vulnerabilidad.

Abstract

This technical report documents a practical cybersecurity exercise conducted in a controlled environment based on the fictional company CyberFort Technologies. The main objective was to analyze the MS17-010 vulnerability, known as EternalBlue, in the SMBv1 protocol of Windows systems through Red Team intrusion testing and to develop containment strategies from the Blue Team perspective. Specialized tools such as Nmap were used for port scanning and vulnerability detection, as well as Metasploit Framework for remote exploitation of the flaw, which allowed privileged system access and exposed critical risks of full control by the attacker.

The report highlights the importance of identifying vulnerabilities through penetration testing techniques to strengthen information security, thereby preventing potential breaches that compromise the confidentiality, integrity, and availability of digital assets. The defense phase included immediate actions such as isolating the compromised system, removing malicious accounts, and proposing hardening measures like disabling the vulnerable protocol, applying patches, and restricting ports, complemented by monitoring through SIEM tools and intrusion detection systems.

Finally, the study emphasizes the educational and diagnostic value of the exercise for developing technical skills in offensive and defensive security, contributing to organizational maturity and the capacity to respond to real threats. The integration of findings, forensic measures, and recommendations helps strengthen the security posture and resilience of digital infrastructures in current corporate contexts.

Keywords: Cybersecurity, Intrusion, Mitigation, Red Team, Vulnerability.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

El presente informe técnico ha sido elaborado por Alonso Dueñas Vaca con el propósito de documentar las acciones realizadas durante las etapas de ejecución de pruebas de intrusión (Red Team) y contención de ataques informáticos (Blue Team), llevadas a cabo en un entorno controlado, tomando como base a la empresa ficticia CyberFort Technologies, como parte de un ejercicio especializado en ciberseguridad ofensiva y defensiva.

Las actividades permitieron simular incidentes reales, aplicando técnicas de escaneo, explotación de vulnerabilidades y posterior contención, todo bajo un enfoque integral que incluyó herramientas reconocidas como Nmap, Metasploit Framewor, además de lineamientos basados en marcos legales y normativos como los controles CIS v8.1.

Este informe adquiere alta relevancia para los analistas senior, ya que expone procedimientos y evidencias detalladas sobre la explotación de vulnerabilidades críticas como MS17-010, así como las estrategias de mitigación implementadas. El documento fortalece la toma de decisiones en entornos corporativos al ofrecer un panorama técnico claro sobre amenazas actuales, metodologías de defensa proactiva y medidas efectivas de respuesta ante incidentes.

Descripción del problema

En el entorno simulado de CyberFort Technologies, se identificó una vulnerabilidad crítica en el protocolo SMBv1 del sistema operativo Windows, específicamente relacionada con la falla MS17-010, también conocida como EternalBlue. Esta amenaza permitió la ejecución remota de código sin autenticación previa, lo que representa un riesgo elevado de intrusión externa.

La falla fue detectada a través de un escaneo de red realizado con Nmap, que reveló el puerto 445 abierto en una máquina con dirección IP 192.168.56.10. Posteriormente, se validó la vulnerabilidad mediante Metasploit Framework, logrando establecer una sesión remota con privilegios de sistema en el equipo comprometido.

Esta situación tuvo consecuencias potencialmente graves para la empresa ficticia, tales como el control total del sistema por parte del atacante, la creación de usuarios con privilegios de administrador, y la posibilidad de instalar puertas traseras, todo lo cual compromete seriamente la confidencialidad, integridad y disponibilidad de los activos digitales de la organización.

Planteamiento del problema

Durante la ejecución de las pruebas de intrusión en un entorno controlado tipo Red Team, se evidenció una situación crítica: la presencia de una vulnerabilidad conocida (MS17-010) en el protocolo SMBv1, que permitía la ejecución remota de código y el control total del sistema sin necesidad de autenticación. Esta falla no solo facilitó el acceso privilegiado al sistema objetivo, sino que también posibilitó la creación de cuentas con permisos administrativos, lo que demuestra un escenario realista de compromiso total de la infraestructura.

Esta situación afecta directamente a la infraestructura y seguridad de la empresa al poner en riesgo la integridad, disponibilidad y confidencialidad de sus sistemas. Una brecha como esta puede ser explotada por atacantes reales para instalar malware, robar información sensible o interrumpir operaciones críticas. La existencia de servicios expuestos sin los debidos parches y controles de seguridad revela una arquitectura débil y mal gestionada, propensa a ataques cibernéticos que podrían tener consecuencias financieras, legales y reputacionales para la organización.

Identificar y resolver esta problemática resulta esencial por varias razones. Primero, permite eliminar vectores de ataque conocidos y prevenir su aprovechamiento por actores maliciosos. Segundo, impulsa la adopción de buenas prácticas de seguridad como la hardenización del sistema, el monitoreo proactivo mediante SIEM, y el cumplimiento de marcos de control como CIS. Por último, fortalece las capacidades del equipo Blue Team para detectar, contener y responder eficazmente ante incidentes de seguridad, garantizando así una postura defensiva robusta y resiliente frente a las amenazas actuales.

Sistematización del problema

Tabla 1

Sistematización del problema en entorno Red Team y acciones Blue Team

Elemento	Contenido
Pregunta principal	¿Cómo se logró explotar exitosamente la vulnerabilidad MS17-010 en el entorno de pruebas tipo Red Team, y qué acciones se tomaron posteriormente para contener el ataque desde el enfoque del Blue Team?
Subpregunta 1	¿Qué herramientas y técnicas se utilizaron para identificar y explotar la vulnerabilidad del sistema?
Respuesta 1	Se utilizó Nmap para escanear el sistema (con el script --script vuln) y detectar el puerto 445 abierto vulnerable a SMBv1. Posteriormente, se usó Metasploit Framework con el módulo ms17_010_eternalblue_win8 para explotar la vulnerabilidad y obtener acceso remoto con privilegios de sistema.
Subpregunta 2	¿Cuál fue el impacto del ataque y qué nivel de control obtuvo el atacante sobre el sistema comprometido?
Respuesta 2	El ataque permitió ejecución remota de código, escalación de privilegios y control total del sistema. El atacante logró abrir una sesión con privilegios de sistema y creó un usuario con acceso de administrador llamado “AlonsoVaca”.
Subpregunta 3	¿Qué medidas implementó el Blue Team para contener el ataque y prevenir futuras intrusiones?

Respuesta 3	El Blue Team aisló la máquina comprometida, revisó los logs del sistema y firewall, eliminó el usuario malicioso, y propuso acciones de hardenización como desactivar SMBv1, restringir puertos como el 445, aplicar parches de seguridad, y aplicar el principio de mínimos privilegios. También se sugirió implementar herramientas como SIEM, UFW, y Snort en modo IPS.

Nota. *Se presentan las preguntas y respuestas clave obtenidas a partir de la experiencia de ataque y defensa durante un ejercicio de pruebas tipo Red Team, con el fin de analizar la explotación de la vulnerabilidad MS17-010 y las acciones tomadas desde el enfoque Blue Team.*

Justificación

El desarrollo de este análisis representa una contribución integral tanto al fortalecimiento técnico como a la madurez organizacional de CyberFort. Al recrear un entorno controlado de pruebas de penetración y contención de amenazas, se consolidan competencias clave en seguridad ofensiva y defensiva, imprescindibles en un contexto donde los riesgos cibernéticos evolucionan con creciente sofisticación y frecuencia.

La aplicación de herramientas como Nmap y Metasploit permitió detectar vulnerabilidades críticas —como MS17-010— y simular escenarios reales de explotación. Este enfoque práctico no solo reveló debilidades técnicas en sistemas y protocolos, sino que también facilitó el diseño de rutas de escalación de privilegios y ataques dirigidos, aportando insumos concretos para el fortalecimiento de infraestructuras digitales.

Adicionalmente, la fase de contención integró una visión estratégica mediante la implementación de controles técnicos y administrativos, como hardenización, monitoreo con SIEM y gestión de accesos. Estas acciones se articularon con marcos de referencia reconocidos como los Controles CIS, reforzando no solo el aprendizaje técnico, sino también la capacidad de respuesta coordinada ante incidentes reales, donde el tiempo de reacción y la precisión son factores decisivos.

Desde una perspectiva organizacional, el ejercicio aporta un valor sustancial al funcionar como una herramienta de diagnóstico y formación. Permite observar con objetividad el desempeño de los analistas en escenarios críticos, su capacidad de análisis, resolución y uso eficiente de herramientas que son estándar en el sector. Este informe, más allá de su carácter académico, se posiciona como un recurso útil para procesos de selección, evaluación y mejora

continua, contribuyendo a la identificación y fortalecimiento de perfiles preparados para enfrentar los desafíos reales de la ciberseguridad.

Objetivos

Objetivo General

Analizar las vulnerabilidades explotadas en un entorno controlado mediante técnicas de pruebas de intrusión Red Team, y formular estrategias de contención desde el enfoque Blue Team para mitigar riesgos, fortalecer la postura de seguridad y consolidar competencias técnicas en ciberseguridad ofensiva y defensiva.

Objetivos Específicos

Implementar acciones de contención en tiempo real ante ciberataques identificados, incluyendo la desconexión de sistemas comprometidos, análisis de tráfico de red y aplicación de hardenización.

(Blue Team)

Aplicar medidas forenses y legales post-incidente, incluyendo el análisis de logs, la documentación técnica de los vectores de ataque y la preservación de evidencias digitales para su posible uso en auditorías o procesos judiciales.

(Evaluación legal/forense)

Evaluar la efectividad de los controles de seguridad aplicados, utilizando como referencia el marco CIS v8.1 y herramientas SIEM, con el propósito de medir el impacto de las vulnerabilidades explotadas y la eficiencia de las respuestas implementadas.

(Resultados esperados)

Integrar los hallazgos del Red Team, las acciones del Blue Team, los registros forenses y las recomendaciones para mejorar la postura de seguridad de la organización.

(Resultados esperados integrados)

Marco de referencia

Estado del arte

Casos anteriores similares de fuga de información o explotación de vulnerabilidades

En los últimos años, se han registrado múltiples incidentes de seguridad que evidencian la importancia de una defensa cibernética robusta:

- **MOAB (Mother of All Breaches)**: En 2024, se descubrió una base de datos con más de 26 mil millones de registros filtrados, incluyendo información de usuarios de plataformas como Twitter, Dropbox y LinkedIn. Esta recopilación masiva de datos comprometidos resalta la magnitud de las brechas de seguridad actuales (Cybernews, 2024).
- **Ataque al Deportivo de La Coruña**: En mayo de 2025, el club español sufrió un ciberataque que comprometió una de sus bases de datos, permitiendo el acceso no autorizado a información identificativa y de contacto de los afectados. El ataque se originó por una brecha de seguridad en su servidor alojado en Amazon Web Services (AWS) (AS, 2025).
- **Explotación de la vulnerabilidad CVE-2024-4577**: Un día después de su divulgación, se observaron numerosos intentos de explotación de esta vulnerabilidad en PHP, demostrando la rapidez con la que los atacantes aprovechan nuevas debilidades (Akamai, 2024).

Referentes técnicos utilizados (herramientas, técnicas, metodologías)

Las prácticas actuales en ciberseguridad se apoyan en diversas herramientas y metodologías para fortalecer las defensas:

- **Herramientas de código abierto para el Blue Team**: Se destacan herramientas como UFW (Uncomplicated Firewall), Snort en modo IPS y AppArmor/SELinux, que permiten configurar reglas de firewall, detectar y bloquear tráfico malicioso, y restringir acciones de procesos respectivamente (TuxCare, 2025; Chris Titus Tech, 2022).
- **Metodologías de Red Team y Blue Team**: El Red Team se enfoca en realizar evaluaciones ofensivas de ciberseguridad, simulando ataques reales para identificar vulnerabilidades. Por otro lado, el Blue Team se dedica a la defensa, implementando medidas para proteger los sistemas y responder a incidentes (Check Point Software, 2023).
- **Controles CIS v8.1**: Este marco ofrece una guía práctica para mejorar la seguridad de la información, especialmente útil para organizaciones con recursos limitados, ayudando a priorizar acciones como la hardenización, gestión de activos y monitoreo (CIS, 2025).

Marco contextual

Características generales de la organización ficticia CyberFort

CyberFort Technologies es una organización ficticia especializada en ofrecer soluciones de ciberseguridad a empresas de diversos sectores. Su enfoque principal es garantizar la protección de los activos digitales de sus clientes mediante la implementación de estrategias proactivas y reactivas frente a amenazas cibernéticas.

Funciones del equipo de ciberseguridad dentro de la organización

El equipo de ciberseguridad de CyberFort Technologies se divide en dos unidades principales:

- **Red Team**: Encargado de simular ataques cibernéticos para identificar vulnerabilidades en los sistemas y evaluar la eficacia de las defensas existentes. Utilizan técnicas de penetración y explotación para emular posibles escenarios de ataque.
- **Blue Team**: Responsable de la defensa de los sistemas, implementando medidas de seguridad, monitoreando actividades sospechosas y respondiendo a incidentes en tiempo real. Su objetivo es contener y mitigar cualquier amenaza que pueda comprometer la integridad de los sistemas.

Marco teórico

En el desarrollo de las pruebas de intrusión y contención de ataques, se aplicaron enfoques clásicos y contemporáneos en ciberseguridad, sustentados principalmente en el modelo Red Team vs Blue Team, el Ciclo de Vida del Pentesting y los Controles CIS como pilares de la defensa proactiva.

Desde el enfoque ofensivo (Red Team), se trabajó bajo el ciclo del hacking ético, el cual incluye fases como reconocimiento, escaneo, explotación y post-explotación. Se utilizó la herramienta Nmap para la enumeración y detección de vulnerabilidades, y Metasploit Framework para ejecutar el exploit MS17-010 (EternalBlue), permitiendo la obtención de una sesión Meterpreter con privilegios de sistema (Nmap, 2025; OffSec, 2025).

Desde el enfoque defensivo (Blue Team), se adoptaron estrategias del marco CIS v8.1, centradas en medidas de hardenización de sistemas, aislamiento de amenazas, y el uso de tecnologías como SIEM (Security Information and Event Management). Entre las técnicas específicas aplicadas se destacan:

- **Pentesting**: ejecución controlada de ataques para explotar una vulnerabilidad SMBv1 crítica (MS17-010), mediante Metasploit.
- **Análisis forense básico**: revisión de logs del sistema y firewall para identificar comportamientos anómalos tras la intrusión.
- **Hardenización de sistemas**: desactivación de protocolos obsoletos, restricción de puertos y aplicación de parches de seguridad (NIST, 2025).
- **Contención y respuesta a incidentes**: desconexión de máquinas comprometidas, eliminación de usuarios maliciosos, y ajustes en las reglas del firewall.

Este marco teórico permite integrar habilidades ofensivas y defensivas dentro de un entorno realista, favoreciendo una visión completa del ciclo de vida de los ciberataques y su prevención.

Marco conceptual

A continuación, se listan los conceptos clave:

- **Pentesting (Pruebas de penetración)**: Es una evaluación de seguridad autorizada que simula ataques reales para identificar y explotar vulnerabilidades en sistemas, redes o aplicaciones, con el fin de mejorar la postura de seguridad de una organización (Cloudflare, 2025).
- **Exploit**: Es un fragmento de código o software que aprovecha una vulnerabilidad específica en un sistema informático para ejecutar acciones no autorizadas, como la instalación de malware o el acceso no permitido a datos sensibles (Cisco, 2025).
- **Escalación de privilegios**: Es una técnica mediante la cual un atacante obtiene niveles de acceso más altos en un sistema, superando las restricciones de seguridad iniciales, ya sea mediante vulnerabilidades en el software o errores de configuración (CrowdStrike, 2025).
- **Shell / Meterpreter**: Una shell es una interfaz que permite la ejecución de comandos en un sistema operativo. Meterpreter es una avanzada shell incluida en el framework Metasploit, que opera en memoria y proporciona capacidades extensibles para realizar tareas de post-explotación en sistemas comprometidos (OffSec, 2025).
- **SIEM (Security Information and Event Management)**: Es una solución que centraliza, analiza y correlaciona eventos de seguridad provenientes de diversas fuentes dentro de una infraestructura de TI, facilitando la detección y respuesta ante incidentes de seguridad (IBM, 2025).
- **Hardenización de sistemas**: Proceso de fortalecer la seguridad de un sistema mediante la reducción de su superficie de ataque, lo que incluye la desactivación de servicios

innecesarios, la aplicación de parches de seguridad y la configuración adecuada de los sistemas (NIST, 2025).

- **IDS / IPS (Intrusion Detection/Prevention Systems)**: Los sistemas de detección de intrusiones (IDS) monitorean el tráfico de red en busca de actividades sospechosas, generando alertas cuando se detectan posibles amenazas. Los sistemas de prevención de intrusiones (IPS), además de detectar, pueden bloquear o prevenir automáticamente dichas amenazas (Juniper Networks, 2025).

Marco normativo

Durante la elaboración de las pruebas y las estrategias de contención, se tomaron como referencia las siguientes normativas y estándares:

- **ISO/IEC 27001**: Sistema de Gestión de Seguridad de la Información (SGSI). Sirvió de guía general para estructurar las fases del pentesting, manejo de incidentes y documentación del proceso (ISO, 2022).
- **ISO/IEC 27002**: Código de buenas prácticas para controles de seguridad. Proporcionó lineamientos clave sobre hardenización, gestión de usuarios y control de accesos (ISO, 2022).
- **Ley 1581 de 2012 (Colombia)**: Régimen general de protección de datos personales. Se consideró para evitar el manejo indebido de datos durante las fases de análisis y explotación.
- **Controles CIS v8.1**: Proporcionan un conjunto de prácticas recomendadas para proteger sistemas y datos contra amenazas comunes. Se utilizaron como marco operativo para la implementación de controles de seguridad durante la fase defensiva del proyecto. Entre

los controles aplicados se encuentran: el inventario y control de activos de hardware y software (Control 1 y 2), la configuración segura de sistemas (Control 4), el control de privilegios administrativos (Control 5) y la protección de datos (Control 3) (CIS, 2025).

- **Ley 1273 de 2009 (Colombia):** Esta ley define delitos informáticos y protege la integridad de los sistemas informáticos y los datos. En este proyecto se consideraron sus disposiciones para garantizar que todas las pruebas ofensivas estuvieran autorizadas y documentadas, sin vulnerar sistemas externos o datos reales de terceros (Congreso de Colombia, 2009).
- **Ley 1621 de 2013 (Colombia)**: Regula la actividad de inteligencia y contrainteligencia del Estado. Aunque está enfocada en la seguridad nacional, establece principios de proporcionalidad y necesidad que también pueden considerarse en ejercicios éticos de seguridad ofensiva dentro de un marco académico y controlado (Congreso de Colombia, 2013).

Metodología

Método

Para el desarrollo de este proyecto se aplicó un enfoque técnico centrado en pruebas de penetración (pentesting) y respuesta ante incidentes dentro de un entorno controlado. Inicialmente, se llevó a cabo un ejercicio de Red Team para identificar, analizar y explotar vulnerabilidades presentes en la red objetivo, específicamente un sistema Windows vulnerable al exploit MS17-010 (EternalBlue). Este proceso incluyó el escaneo y reconocimiento de servicios, explotación de vulnerabilidades y evaluación del impacto asociado a los ataques ejecutados. Posteriormente, se implementaron técnicas de Blue Team orientadas a la contención y mitigación en tiempo real del ataque detectado. Esto implicó el análisis de la situación mediante inspección de logs y tráfico de red, uso de herramientas libres para el aislamiento de la máquina comprometida y la hardenización de sistemas para reducir la superficie de ataque, todo bajo un enfoque reactivo y de fortalecimiento continuo de la postura de seguridad.

Tipo de estudio

El presente trabajo corresponde a un estudio exploratorio y descriptivo de carácter técnico-práctico. Exploratorio porque se buscó descubrir y comprender las vulnerabilidades existentes en un sistema objetivo y las vías de explotación; descriptivo porque se documentaron con detalle las acciones, herramientas, resultados y estrategias para la contención y mitigación de las amenazas detectadas durante el proceso.

Recolección de datos

La recolección de información técnica se llevó a cabo mediante diversas herramientas especializadas de código abierto y licencia GPL, orientadas al análisis, escaneo, explotación y monitoreo de la red y sistemas involucrados. Entre las principales fuentes y herramientas utilizadas se destacan:

- **Nmap**: para realizar escaneos de puertos y detección de vulnerabilidades específicas mediante scripts (--script vuln). Proporcionó datos sobre servicios activos y puertos abiertos, como el puerto 445 (SMB).
- **Metasploit Framework**: para la explotación controlada de vulnerabilidades, permitiendo obtener acceso con privilegios elevados y ejecutar comandos remotos, como la creación de usuarios con privilegios administrativos.
- **Herramientas de hardenización y monitoreo** como **UFW (Uncomplicated Firewall)**, **Snort (en modo IPS)** y **AppArmor/SELinux** para implementar políticas de seguridad, bloqueo de tráfico malicioso y control de acceso mandatorio en los sistemas.

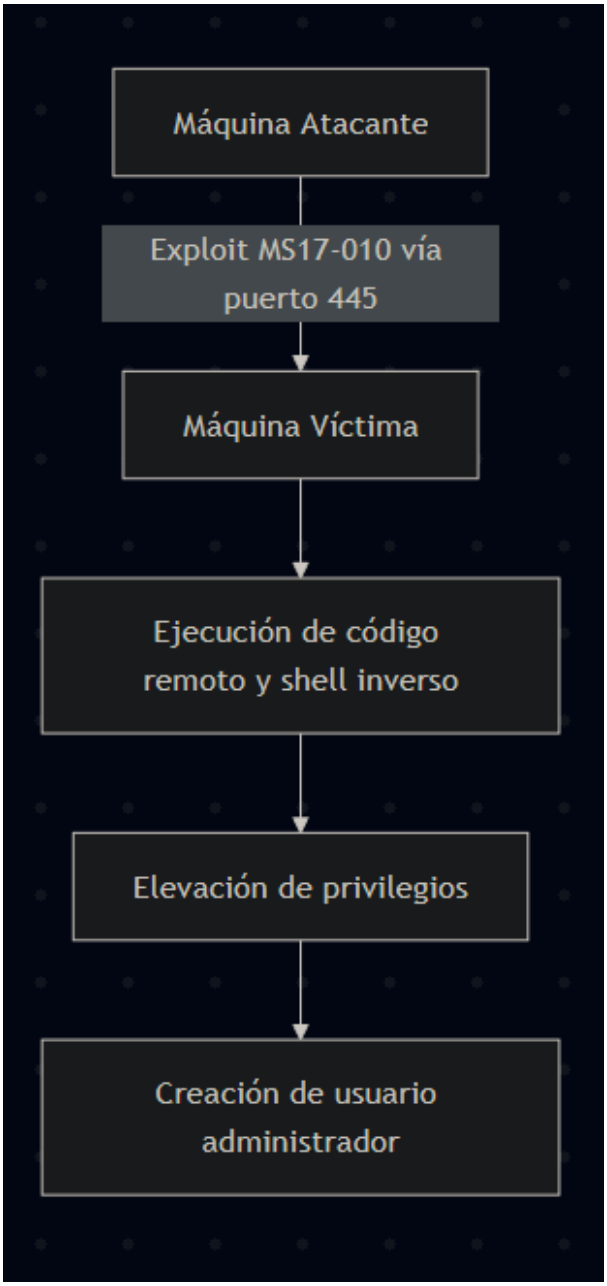
Los datos recolectados incluyeron registros de red, imágenes forenses de los sistemas afectados, resultados de escaneo de vulnerabilidades, logs del sistema operativo y firewall, y evidencias de explotación y mitigación, los cuales fueron documentados para la elaboración de informes técnicos detallados.

Resultados

Primer resultado (Red Team)

Figura 1

Gráfico explicativo del ataque

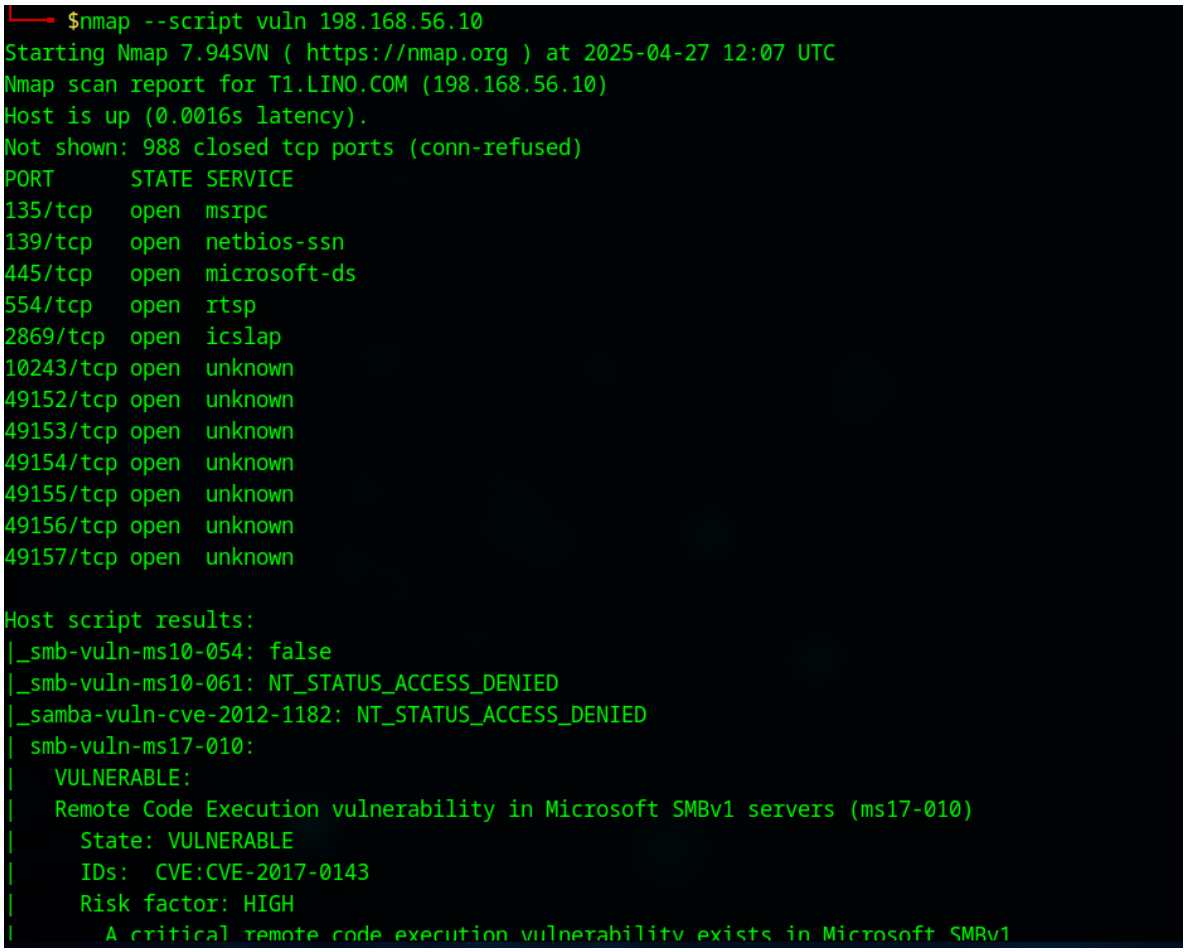


Fuente: elaboración propia

Durante la fase de ataque, se identificó una vulnerabilidad crítica en el servicio SMBv1 del sistema objetivo, específicamente la vulnerabilidad MS17-010 (conocida como EternalBlue), expuesta en el puerto 445.

Figura 2

Imagen del puerto 445 abierto, vulnerabilidad MS17-010.

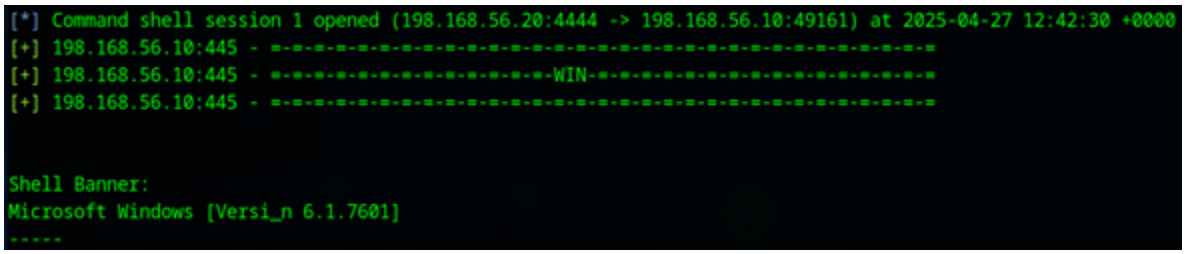


Fuente: elaboración propia

Esta falla permitió la explotación remota del sistema mediante el módulo exploit/windows/smb/ms17_010_eternalblue_win8 de Metasploit Framework. Como resultado, se logró obtener una sesión Meterpreter estable con privilegios de sistema, lo que posibilitó la ejecución de comandos con permisos elevados (ver Apéndice A, Ilustración A1).

Figura 3

Ejecución exitosa del comando exploit/windows/smb/ms17_010_eternalblue_win8



Fuente: elaboración propia.

Aprovechando esta situación, se procedió a crear un usuario con privilegios administrativos (usuario "AlonsoVaca"), confirmando así el control total del sistema comprometido (ver Apéndice A, Ilustraciones A2, A3 y A4).

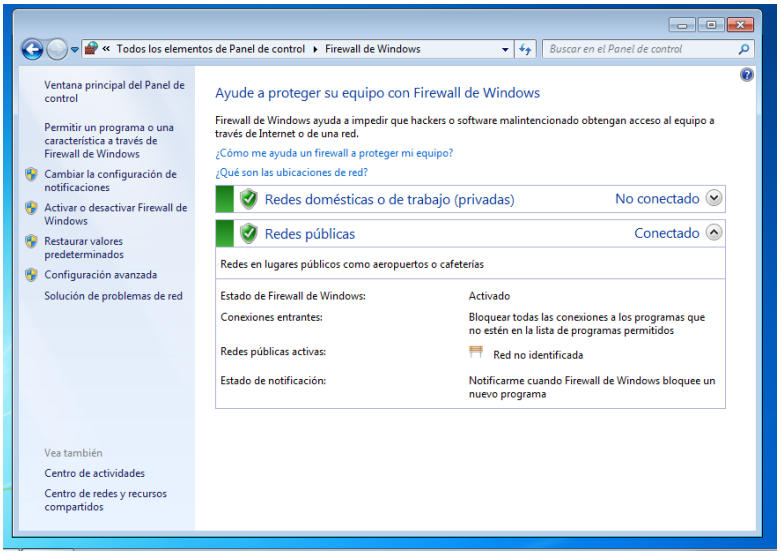
Segundo resultado (Blue Team)

Ante un ataque informático en tiempo real, la prioridad del Blue Team fue contener la amenaza para evitar su propagación y proteger el resto de la infraestructura. La primera acción técnica consistió en aislar la máquina comprometida, desconectándola de la red o deshabilitando su adaptador desde el switch o firewall. Esto permitió detener la actividad maliciosa y evitar movimientos laterales hacia otros dispositivos (Proofpoint, s.f.).

En la fase de recuperación, se implementaron medidas correctivas enfocadas en fortalecer la seguridad del perímetro de red. Entre estas, se configuraron adecuadamente los firewalls para bloquear accesos no autorizados y se aplicaron políticas para restringir puertos críticos, como el 445, utilizado por SMB. También se recomendó la desactivación del protocolo SMBv1, vulnerable y explotado en ataques previos (ver Apéndice B, Ilustraciones B1 y B2), así como la aplicación sistemática de parches y actualizaciones automatizadas para evitar vulnerabilidades conocidas (Microsoft, 2017; Check Point, s.f.).

Figura 4

Configuración de firewalls Windows 7.

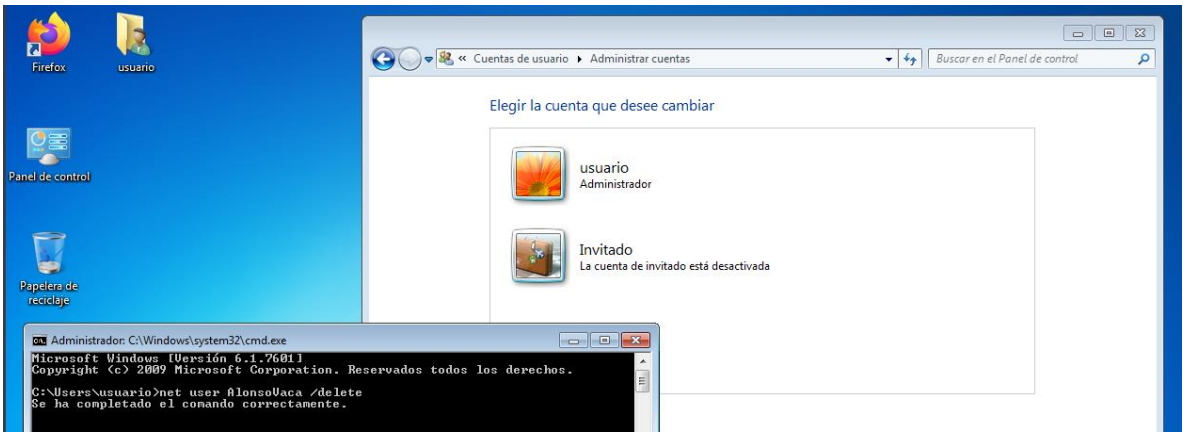


Fuente: elaboración propia

Adicionalmente, como parte de la contención del incidente, se identificó y eliminó la cuenta de usuario maliciosa **"AlonsoVaca"**, creada por el atacante durante la explotación del sistema. Esta acción fue fundamental para revocar el acceso persistente que el adversario había establecido y restablecer el control sobre la máquina comprometida.

Figura 5

Eliminación de la cuenta AlonsoVaca creada en el ataque.



fuente: elaboración propia

Recomendaciones para mitigar daños y prevenir futuros ataques

- Realizar análisis exhaustivos post-incidente utilizando herramientas GPL como Wireshark para captura y análisis de paquetes sospechosos, y Sysinternals para inspección de procesos, puertos y servicios activos.
- Revisar logs del sistema y firewall para detectar patrones anómalos o movimientos laterales.
- Identificar y eliminar cuentas no autorizadas creadas durante el ataque, como la cuenta ficticia *AlonsoVaca*, para eliminar accesos persistentes.
- Deshabilitar protocolos inseguros, como SMBv1, para eliminar vectores de ataque ampliamente explotados.
- Aplicar políticas de parcheo automatizadas para mantener los sistemas actualizados con los últimos fixes de seguridad.
- Configurar reglas estrictas en firewalls para restringir el acceso a puertos críticos, principalmente el puerto 445.

- Implementar el principio de privilegios mínimos en usuarios y servicios.
- Utilizar herramientas de contención en tiempo real como Firewall UFW, Snort en modo IPS, y AppArmor o SELinux para limitar el daño y movimientos laterales.
- Monitorear continuamente los logs y procesos para detectar anomalías en tiempo real.

Conclusiones

El proceso combinado de Red Team y Blue Team en el ejercicio realizado permitió profundizar en el entendimiento práctico y teórico sobre la gestión de incidentes y seguridad informática en un entorno controlado. Entre los aprendizajes clave se destacan:

- La necesidad de un enfoque dual: mientras el Red Team se enfoca en detectar y explotar vulnerabilidades (como la crítica en SMBv1 MS17-010), el Blue Team debe actuar de forma inmediata y coordinada para contener el ataque, limitar el daño y fortalecer la infraestructura mediante medidas de hardenización.
- La práctica del pentesting evidenció cómo sistemas sin parches ni configuraciones adecuadas son extremadamente vulnerables a ataques que pueden derivar en el control total del sistema, incluyendo la creación de usuarios con privilegios administrativos no autorizados.
- La contención efectiva requiere no solo de herramientas técnicas, sino también de protocolos claros, monitoreo constante y trabajo colaborativo entre equipos de seguridad.

En cuanto al estado general de la ciberseguridad en CyberFort Technologies, las pruebas revelaron:

- La presencia de vulnerabilidades críticas conocidas y explotables demuestra una brecha importante en la gestión de parches y actualización de sistemas.

- La infraestructura presenta una superficie de ataque considerable que debe ser reducida mediante políticas de hardenización, desactivación de servicios inseguros (como SMBv1) y restricciones estrictas en la red (por ejemplo, bloqueo del puerto 445 en firewalls).
- La implementación de estándares como los Controles CIS y la incorporación de sistemas SIEM pueden optimizar la detección y respuesta ante incidentes, especialmente en un contexto con recursos limitados.
- La cultura de seguridad debe fortalecerse con entrenamientos constantes y la adopción de buenas prácticas que permitan a CyberFort evolucionar hacia un modelo de defensa proactiva y resiliente.

El ejercicio destacó la crítica necesidad de mantener una postura de seguridad actualizada y vigilante, donde tanto la identificación temprana de amenazas como la rápida contención son pilares indispensables para salvaguardar la integridad y continuidad operativa de CyberFort Technologies.

Recomendaciones

Desactivar protocolos inseguros y vulnerables

- Deshabilitar SMBv1 en todos los sistemas Windows, ya que esta versión es ampliamente conocida por vulnerabilidades críticas como MS17-010 (EternalBlue).
- Revisar regularmente las configuraciones de protocolos de red para evitar que versiones obsoletas y no seguras permanezcan activas.

Implementar un proceso de parcheo y actualización automatizado

- Establecer políticas de actualización automática o con revisión periódica para sistemas operativos, aplicaciones y servicios críticos.
- Priorizar la instalación de parches de seguridad que corrijan vulnerabilidades explotables remotamente.

Fortalecer las reglas de firewall y segmentación de red

- Bloquear puertos no esenciales, en particular el puerto 445 (SMB) para accesos externos y restringirlo solo para comunicaciones internas confiables.
- Implementar segmentación de red para aislar sistemas críticos y limitar movimientos laterales ante compromisos internos.

Aplicar el principio de mínimos privilegios

- Revisar y restringir las cuentas de usuario y sus permisos, evitando que usuarios tengan privilegios administrativos innecesarios.
- Controlar estrictamente la creación y modificación de cuentas con privilegios elevados.

Implementar sistemas de monitoreo y detección basados en herramientas libres

- Instalar y configurar un SIEM open source o gratuito (ejemplo: ELK Stack, Wazuh) para centralizar logs y detectar comportamientos anómalos en tiempo real.
- Usar IDS/IPS libres como Snort o Suricata para detectar y bloquear tráfico malicioso.

Hardenización de sistemas operativos

- Aplicar políticas de hardening como deshabilitar servicios innecesarios, restringir acceso a recursos críticos y aplicar controles de acceso mandatorios (AppArmor o SELinux).
- Realizar revisiones periódicas de la configuración de seguridad.

Capacitación continua del personal

- Entrenar al equipo técnico en prácticas de seguridad, reconocimiento de vectores de ataque y respuesta ante incidentes.
- Simular ataques controlados periódicamente (pentesting y ejercicios Red Team/Blue Team) para evaluar y mejorar la postura defensiva.

Procedimientos claros para respuesta a incidentes

- Definir protocolos para aislamiento rápido de sistemas comprometidos, análisis de logs y recuperación segura.
- Contar con una comunicación efectiva entre Blue Team, respuesta a incidentes y áreas técnicas.

Auditorías y pruebas periódicas de seguridad

- Realizar auditorías internas y externas para verificar el cumplimiento de políticas de seguridad y detectar nuevas vulnerabilidades.
- Usar escaneos regulares con Nmap y herramientas de análisis de vulnerabilidades para mantener la visibilidad del estado del sistema.

Referencias Bibliográficas

Akamai. (2024). *CVE-2024-4577 Exploits in the Wild One Day After Disclosure*. https://www.akamai.com/blog/security-research/2024-php-exploit-cve-one-day-after-disclosure

AS. (2025). *Ciberataque al Depor*. https://as.com/futbol/segunda/ciberataque-al-depor-n/

Check Point. (s.f.). *Las 6 fases de un plan de respuesta a incidentes*. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-incident-response/the-6-phases-of-an-incident-response-plan/

Check Point Software. (2023). *Red Team vs. Blue Team*. https://www.checkpoint.com/cyber-hub/cyber-security/red-team-vs-blue-team/

Cisco. (2025). *What Is an Exploit?*. https://www.cisco.com/site/us/en/learn/topics/security/what-is-an-exploit.html

Cloudflare. (2025). *What is penetration testing?*. https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

Congreso de Colombia. (2009). *Ley 1273 de 2009*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34943

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

Congreso de Colombia. (2013). *Ley 1621 de 2013*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53100

Chris Titus Tech. (2022). *The 3 Biggest Security Mistakes Linux Users Make*. https://christitus.com/linux-security-mistakes/

CIS. (2025). *CIS Critical Security Controls Version 8.1*. https://www.cisecurity.org/controls/v8-1

CrowdStrike. (2025). *What is Privilege Escalation?*. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/privilege-escalation/

CyberArk. (s.f.). *¿Qué es el mínimo privilegio? - Definición*. https://www.cyberark.com/es/what-is/least-privilege/

Cybernews. (2024). *Mother of all breaches reveals 26 billion records*. https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/

Forlopd. (s.f.). *Actualizaciones de Software y Parches de Seguridad: Por Qué son Cruciales*. https://forlopd.es/actualizaciones-de-software-y-parches-de-seguridad-por-que-son-cruciales/

Gomez, A. (2020). *Red Team operations and cybersecurity defense*. Cybersecurity Press.

IBM. (2025). *What is SIEM?*. https://www.ibm.com/think/topics/siem

ISO. (2022). *ISO/IEC 27001:2022 & ISO/IEC 27002:2022 Information security standards*. https://www.iso.org/standard/27001

Juniper Networks. (2025). *What is IDS and IPS?*. https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

LevelBlue. (2020). *Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux*. https://levelblue.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

Microsoft. (2017). *Microsoft Security Bulletin MS17-010 - Critical*. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Nationwide. (s.f.). *Cómo capacitar a los empleados sobre ciberseguridad*. https://espanol.nationwide.com/business/solutions-center/cybersecurity/train-employees

NIST. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2025). *Hardening*. https://csrc.nist.gov/glossary/term/hardening

Nmap. (2025). *smb-vuln-ms17-010 NSE script*. https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html

Nmap. (s.f.). *Guía de referencia de Nmap (Página de manual)*. https://nmap.org/man/es/index.html

OffSec. (2025). *Meterpreter Basics - Metasploit Unleashed*. https://www.offsec.com/metasploit-unleashed/meterpreter-basics/

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. NIST Special Publication 800-94. https://doi.org/10.6028/NIST.SP.800-94

Stallings, W. (2018). *Network security essentials: Applications and standards* (6th ed.). Pearson.

TuxCare. (2025). *25+ Essential Linux Security Tools: Key Features, Uses & More*. https://tuxcare.com/blog/linux-security-tools/

TuxCare. (s.f.). *AppArmor vs SELinux: Comparación de las diferencias*. https://tuxcare.com/es/blog/selinux-vs-apparmor/

Wazuh. (s.f.). *Wazuh - Open Source XDR. Open Source SIEM*. https://wazuh.com/

Whitman, M., & Mattord, H. (2018). *Principles of information security* (6th ed.). Cengage Learning.

Zscaler. (s.f.). *¿Qué es la segmentación de red? - Definición y casos prácticos*. https://www.zscaler.com/es/resources/security-terms-glossary/what-is-network-segmentation

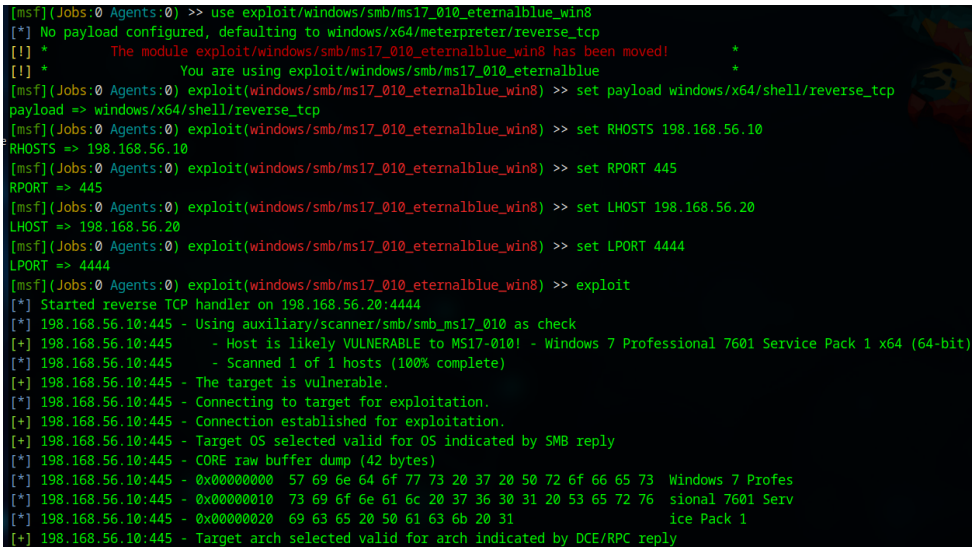
Apéndices

Apéndice A

Figura A1

Explotación con Metasploit, ejecución del comando

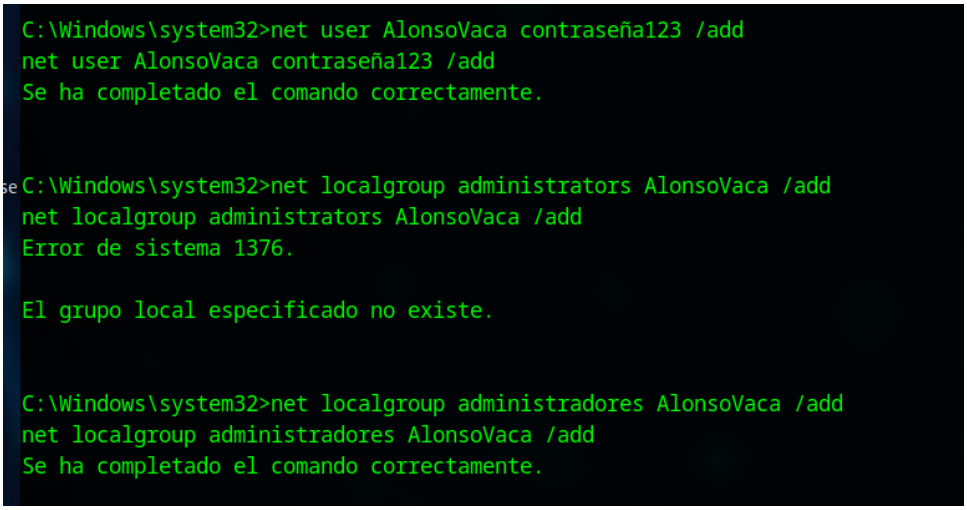
mexploit/windows/smb/ms17_010_eternalblue_win8.



Fuente: elaboración propia

Figura A2

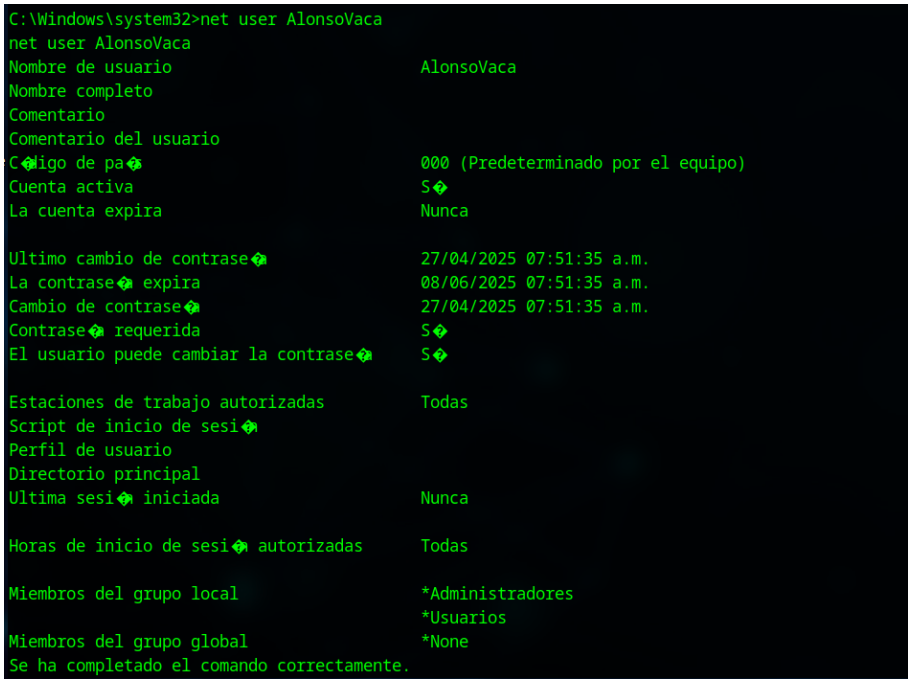
Creación de cuenta en la maquina victima



Fuente: elaboración propia

Figura A3

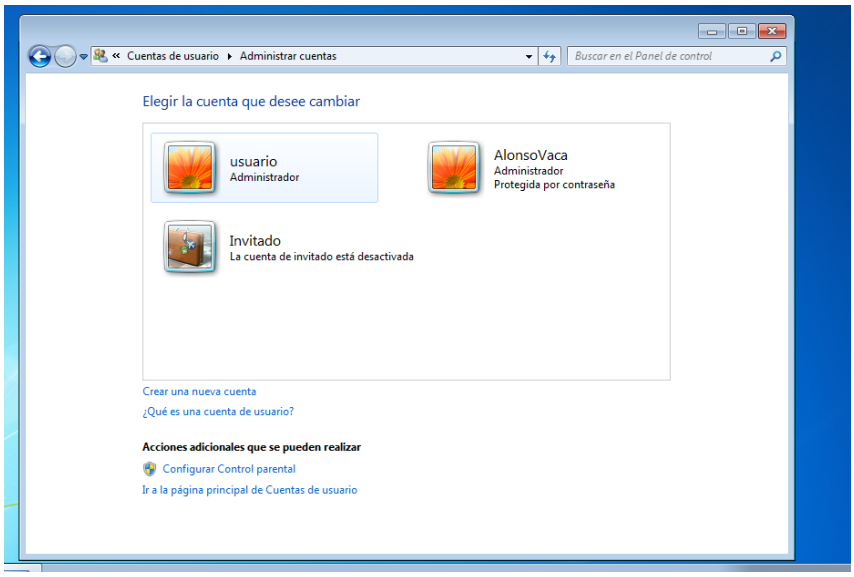
Comprobación de la creación desde la maquina atacante.



Fuente: elaboración propia.

Figura A4

Comprobación de la creación desde la maquina víctima.

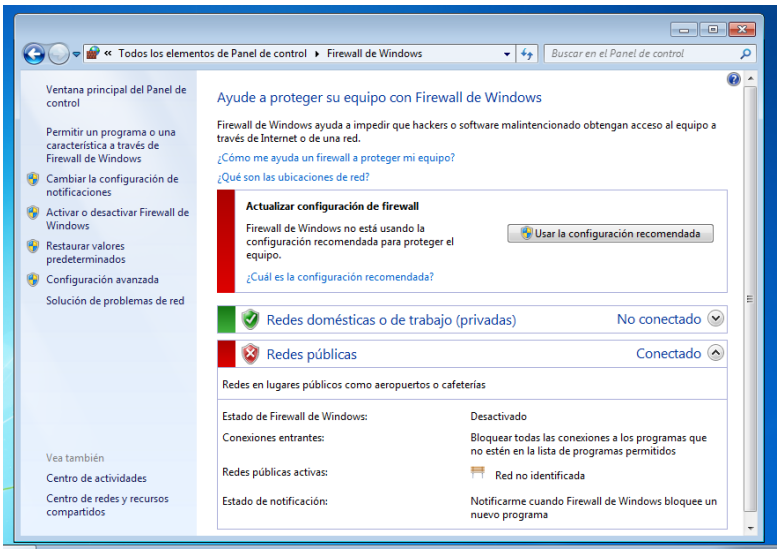


Fuente: elaboración propia.

Apéndice B

Figura B1

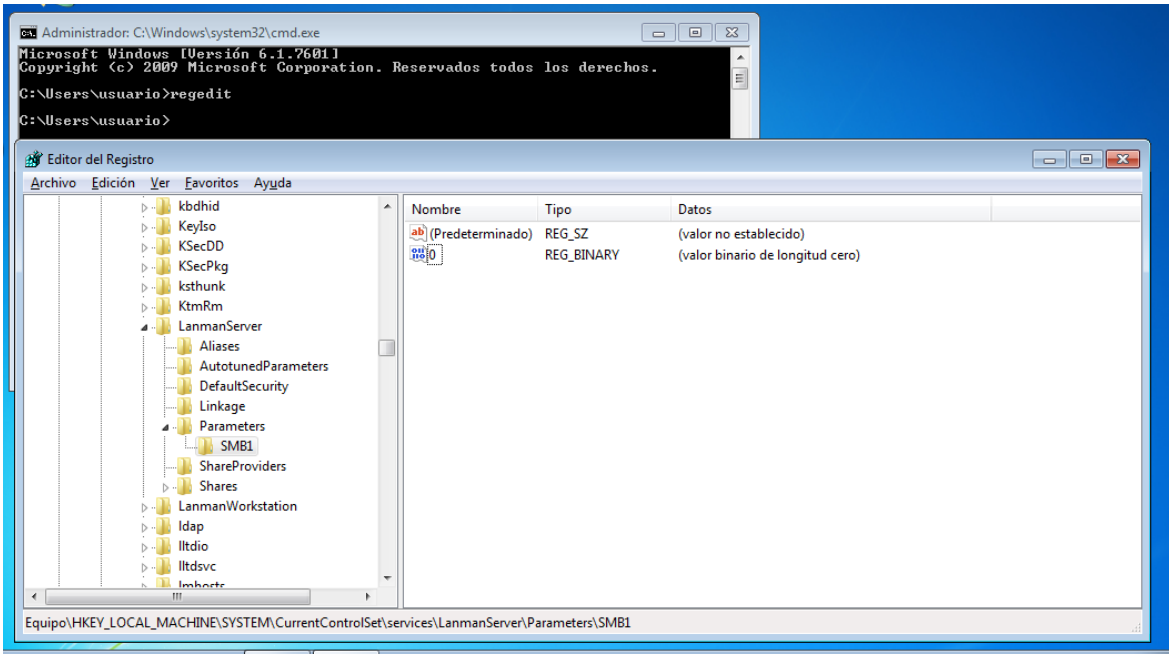
Firewalls Windows 7 desconfigurados.



Fuente: elaboración propia

Figura B2

Desactivación de SMB1, Windows 7.



Fuente: elaboración propia

SUSTENTACION

LINK:

YOUTUBE:

https://www.youtube.com/watch?v=7dezGC3_bgU

https://youtu.be/7dezGC3_bgU

ONEDRIVE:

FASE 5 ENTREGA FINAL.mp4

RESULTADO DE PRUEBA ANTI PLAGIO