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

Andres Santiago Torres Caceres

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Seminario Especializado: Equipos Estratégicos en Ciberseguridad:

Red Team & Blue Team

2025

Resumen

Este informe presenta los aprendizajes y actividades del seminario “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, centrado en la simulación de ataques y estrategias de defensa organizacional. Se desarrollaron ejercicios prácticos de pentesting con herramientas como Nmap, Metasploit y OpenVAS, permitiendo identificar vulnerabilidades y aplicar medidas de contención.

El trabajo integró conocimientos técnicos con marcos normativos como la Ley 1273 de 2009, la Ley 1581 de 2012, y estándares internacionales como ISO 27001 y los CIS Benchmarks. También se reflexionó sobre dilemas éticos y legales en ciberseguridad, abordando prácticas empresariales que podrían cruzar límites legales.

Finalmente, se incluyó el desarrollo de un trabajo independiente orientado al fortalecimiento de competencias en seguridad digital, el uso de herramientas especializadas y el análisis crítico sobre la legalidad y ética de ciertas acciones en entornos digitales.

Palabras clave. Ciberseguridad, Pentesting, Protección, Seguridad digital, Vulnerabilidades

Abstract

This report presents the learnings and activities of the seminar "Strategic Teams in Cybersecurity: Red Team & Blue Team", focused on the simulation of attacks and organizational defense strategies. Practical pentesting exercises were developed with tools such as Nmap, Metasploit and OpenVAS, allowing to identify vulnerabilities and apply containment measures.

The work integrated technical expertise with regulatory frameworks such as Law 1273 of 2009, Law 1581 of 2012, and international standards such as ISO 27001 and CIS Benchmarks. It also reflected on ethical and legal dilemmas in cybersecurity, addressing business practices that could cross legal boundaries.

Finally, it included the development of independent work aimed at strengthening skills in digital security, the use of specialized tools and critical analysis on the legality and ethics of certain actions in digital environments.

Keywords. Cybersecurity, Digital Security, Pentesting, Protection, Vulnerabilities

Contenido

Lista de Figuras

Glosario

Benchmarks CIS. Guías de configuración segura para sistemas operativos, software y hardware, que proporcionan recomendaciones detalladas para minimizar vulnerabilidades.
(Center for Internet Security, 2025)

Common Vulnerabilities and Exposures (CVE). Sistema estandarizado gestionado por MITRE para identificar y catalogar vulnerabilidades en software y hardware.
(MITRE, s. f.)

Dradis Framework. Herramienta utilizada para organizar y presentar informes técnicos de seguridad de manera profesional.
(CSIRT Académico UNAD, s. f.)

EDR (Endpoint Detection and Response). Solución de seguridad avanzada que permite detectar, investigar y responder a amenazas en dispositivos finales.
(Gorman, 2023)

Escalada de privilegios. Técnica que permite a un atacante obtener mayores permisos dentro de un sistema comprometido.
(Herzog, 2010)

Exploit. Código o técnica que aprovecha una vulnerabilidad específica para comprometer un sistema.
(Ciberseguridad Red Team, 2025)

Explotación. Fase del pentesting en la que se aprovechan vulnerabilidades para obtener acceso no autorizado a sistemas.
(CEH v11, s. f.)

Metasploit Framework. Plataforma modular de código abierto para ejecutar exploits y simular ataques cibernéticos.

(Rapid7, s. f.)

Mimikatz. Herramienta utilizada para obtener credenciales y realizar escalada de privilegios en sistemas Windows.

(Herzog, 2010)

Nmap (Network Mapper). Herramienta de escaneo de redes que permite identificar dispositivos, puertos abiertos y servicios activos.

(Nmap.org, s. f.)

Open Source Intelligence (OSINT). Técnicas de recopilación de información a partir de fuentes públicas.

(NIST SP 800-115, 2020)

OpenVAS. Sistema de análisis de vulnerabilidades de código abierto mantenido por Greenbone Networks.

(Greenbone, s. f.)

Pentesting (Pruebas de penetración). Simulación controlada de ataques para evaluar la seguridad de sistemas informáticos.

(CSIRT Académico UNAD, s. f.)

PoC (Proof of Concept). Demostración práctica que valida la existencia y explotabilidad de una vulnerabilidad, como la creación de un usuario administrador.

(Ciberseguridad Red Team, 2025)

Introducción

El presente informe técnico recoge las actividades y conocimientos adquiridos durante el seminario especializado “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, cuyo objetivo fue proporcionar una comprensión profunda de las estrategias de ataque y defensa en ciberseguridad. A través de ejercicios prácticos, se simularon escenarios de ciberataques y se implementaron medidas de protección para mejorar la seguridad organizacional. Además, se exploraron aspectos clave como las fases del pentesting, el uso de herramientas especializadas y el análisis de vulnerabilidades.

Este informe también reflexiona sobre la importancia del cumplimiento normativo y las mejores prácticas internacionales, al tiempo que aborda los dilemas éticos y legales derivados de las actividades cibernéticas. El trabajo pretende contribuir al desarrollo de competencias técnicas y legales en el ámbito de la ciberseguridad, promoviendo un enfoque integral y responsable frente a los desafíos del entorno digital.

Justificación

La creciente sofisticación de los ciberataques y la constante evolución de las amenazas digitales hacen que la ciberseguridad sea un área crítica para proteger la integridad de las organizaciones y los datos que gestionan. El seminario “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team” se diseñó para proporcionar una formación integral que combine tanto la perspectiva ofensiva como defensiva de la seguridad cibernética.

Este informe se justifica en la necesidad de formar profesionales capaces de identificar y mitigar vulnerabilidades a través de simulaciones de ataques reales, así como de aplicar las mejores prácticas en la defensa de infraestructuras digitales. Asimismo, la integración de marcos legales y normativos como la Ley 1273 de 2009 y la Ley 1581 de 2012, junto con estándares internacionales, refuerza la importancia de abordar la ciberseguridad desde una perspectiva ética y legal. La implementación de estas herramientas y estrategias en entornos controlados permite no solo mejorar las competencias técnicas, sino también reflexionar sobre las implicaciones legales y éticas que implica el ejercicio de la ciberseguridad en el ámbito digital.

Este informe busca, entonces, contribuir al desarrollo de habilidades clave en los campos de la ciberseguridad y la legislación informática, promoviendo un enfoque integral y responsable frente a los retos de seguridad que enfrentan las organizaciones en la actualidad.

Objetivos

Objetivo General

Analizar integralmente las prácticas operativas y estratégicas de los equipos Red Team y Blue Team, evaluando su conformidad con los principios éticos y las normativas legales vigentes en Colombia, con el fin de identificar riesgos legales y éticos, y proponer mejoras que fortalezcan la efectividad técnica de las acciones de ciberseguridad en armonía con los marcos normativos y estándares internacionales.

Objetivos Específicos

Analizar las prácticas realizadas por los equipos de Red Team y Blue Team, evaluando su alineación con los principios éticos en el contexto de la ciberseguridad.

Evaluar el cumplimiento de las normativas legales vigentes durante las actividades de pentesting y defensa.

Identificar posibles riesgos legales y éticos derivados de las estrategias y tácticas empleadas en la simulación de ciberataques y medidas de defensa.

Proponer mejoras en las prácticas de ciberseguridad que optimicen tanto la efectividad técnica como el cumplimiento con las normativas legales y los estándares éticos internacionales.

Etapa 1 Conceptos Equipos De Seguridad

Legislación Vigente En Colombia Sobre Delitos Informáticos Y Protección De Datos Personales

Colombia ha consolidado un marco normativo robusto orientado a regular tanto los delitos informáticos como la protección de los datos personales, en respuesta al crecimiento exponencial del uso de las tecnologías de la información y las comunicaciones (TIC). Esta evolución legislativa ha sido impulsada por la necesidad de proteger los activos digitales, prevenir el uso indebido de sistemas tecnológicos y garantizar los derechos fundamentales de los ciudadanos en el entorno digital. En este contexto, el ordenamiento jurídico colombiano se ha fortalecido con la promulgación de diversas leyes que articulan un sistema de defensa frente a las amenazas cibernéticas y establecen parámetros claros para el tratamiento de datos personales (Congreso de Colombia, 2009; 2012).

1. Ley 1273 De 2009 – Delitos Informáticos

La Ley 1273 de 2009 introdujo modificaciones al Código Penal colombiano mediante la creación del Título VII BIS, con el propósito de reconocer un nuevo bien jurídico: la protección de la información y de los datos. Esta normativa tipifica como delitos varias conductas asociadas al uso indebido de tecnologías, incluyendo el acceso no autorizado a sistemas informáticos, la obstrucción ilegítima de redes, la interceptación de datos sin permiso, el daño o destrucción de información digital, el uso de software malicioso (malware), y prácticas de engaño como el phishing (Congreso de Colombia, 2009).

Esta ley contempla sanciones que incluyen penas privativas de la libertad que oscilan entre 36 y 120 meses, además de multas que pueden alcanzar hasta 1.500 salarios mínimos mensuales legales vigentes. De manera adicional, incorpora agravantes en situaciones donde las acciones delictivas afecten sistemas críticos del Estado, del sector financiero, o sean cometidas por funcionarios públicos o mediante abuso de confianza (Delta Asesores, 2023).

2. Ley 1581 De 2012 – Protección De Datos Personales

La Ley 1581 de 2012 constituye el marco general para la regulación del tratamiento de datos personales en Colombia. Esta legislación tiene como finalidad asegurar el respeto al derecho fundamental que tienen todas las personas a conocer, actualizar, rectificar y suprimir la información que sobre ellas se almacene en bases de datos administradas por entidades públicas o privadas (Congreso de Colombia, 2012).

Entre los elementos más relevantes de esta ley se destacan:

La necesidad de contar con una autorización previa expresa e informada por parte del titular de los datos.

La aplicación de principios rectores como la legalidad, finalidad, libertad, veracidad, transparencia, seguridad, confidencialidad y acceso restringido.

La imposición de obligaciones específicas a los responsables y encargados del tratamiento de datos, como la implementación de políticas internas de protección de datos, la adopción de medidas de seguridad administrativas, técnicas y jurídicas, y la habilitación de canales efectivos de atención para el ejercicio de los derechos de los titulares (Superintendencia de Industria y Comercio, 2013).

3. Ley 1266 De 2008 – Régimen De Habeas Data Financiero

Aunque fue promulgada con un enfoque principal en el ámbito financiero, la Ley 1266 de 2008 también forma parte del engranaje legal que protege los datos personales en Colombia.

Esta norma regula el tratamiento de la información financiera, crediticia, comercial y de servicios almacenada en centrales de riesgo, y reconoce a los titulares el derecho a la veracidad, actualización y supresión de sus datos cuando se identifiquen errores o un uso indebido de los mismos (Congreso de Colombia, 2008). Su objetivo es promover la transparencia y la protección de los derechos de los ciudadanos en el acceso y uso de servicios financieros.

4. Decreto 1377 de 2013 – Reglamentación de la Ley 1581

El Decreto 1377 de 2013 fue expedido con el propósito de facilitar la implementación efectiva de la Ley 1581 de 2012. Este decreto establece lineamientos para recolectar las autorizaciones necesarias en los casos donde estas no hayan sido obtenidas previamente, así como los mecanismos para informar a los titulares sobre el uso y tratamiento de sus datos personales (Presidencia de la República de Colombia, 2013).

Además, este reglamento impone la obligación de registrar las bases de datos ante la Superintendencia de Industria y Comercio (SIC), entidad que actúa como autoridad de vigilancia y control. La SIC tiene la responsabilidad de supervisar el cumplimiento de la normativa en materia de protección de datos, así como de sancionar cualquier incumplimiento.

¿Consideras Que La Legislación Actual En Colombia Es Suficiente Para Enfrentar Las Amenazas Cibernéticas Actuales? ¿Qué Aspectos Deberían Fortalecerse?

Considero que, en Colombia, la legislación sobre delitos informáticos y protección de datos ha avanzado significativamente gracias a leyes como la 1273 de 2009 y la 1581 de 2012, las cuales muestran un esfuerzo por adaptar el marco legal a los desafíos del entorno digital.

Sin embargo, estas normas aún son insuficientes frente a las amenazas cibernéticas actuales, que evolucionan más rápido que la capacidad normativa del país.

Entre los principales desafíos se encuentra la rápida evolución del cibercrimen, la cual exige una actualización constante del marco legal. A esto se suman las deficiencias en la implementación de las normas, ya que muchas entidades, tanto públicas como privadas, no aplican adecuadamente los estándares de seguridad exigidos. Asimismo, la falta de cooperación internacional limita la capacidad del país para enfrentar delitos que trascienden fronteras. Otro reto importante es la escasa cultura de ciberseguridad entre la ciudadanía y en las instituciones, lo cual debilita las estrategias preventivas.

Con el fin de fortalecer el marco, se plantea la necesidad de una modernización y actualización constante de la legislación, que permita responder de manera oportuna a las nuevas formas de ciberdelincuencia. Igualmente, es fundamental destinar mayores recursos a las autoridades competentes, mediante la inversión en tecnología, capacitación y la incorporación de personal especializado. Otro aspecto clave es fomentar la educación en ciberseguridad en todos los niveles.

Etapas Del Pentesting Y Herramientas Asociadas

Las pruebas de penetración, conocidas como pentesting, se desarrollan a través de un conjunto de fases metodológicas orientadas a evaluar la seguridad de los sistemas informáticos. Estas etapas permiten identificar debilidades en una infraestructura tecnológica, simular ataques controlados y proponer medidas correctivas para mejorar la postura de seguridad de una organización (CSIRT Académico UNAD, s. f.)

Planificación O Interacción Inicial

Esta fase consiste en definir el alcance, los objetivos y los límites del proceso de pruebas de penetración. Se establecen los acuerdos legales y éticos que permitirán al auditor trabajar dentro de un marco controlado y autorizado (PTES, 2022).

Herramienta ejemplo: Recon-ng, ideal para la automatización de la recolección inicial de información.

Recolección De Información O Descubrimiento

En esta etapa se recopila información del objetivo utilizando técnicas OSINT (Open Source Intelligence), escaneo de redes y análisis de puertos y servicios activos (NIST SP 800-115, 2020).

Herramienta ejemplo: Nmap, ampliamente utilizada para escanear redes y descubrir servicios disponibles.

Identificación De Vulnerabilidades Y Evaluación De Riesgos

Se analizan los sistemas detectados para identificar vulnerabilidades explotables, utilizando herramientas automatizadas y revisión manual, considerando la criticidad y el impacto potencial (OWASP, s. f.).

Herramienta ejemplo: OpenVAS, útil para análisis de vulnerabilidades a nivel de red y sistemas operativos.

Explotación O Obtención De Acceso

Una vez identificadas las vulnerabilidades, se intenta explotarlas con el fin de obtener acceso al sistema. Esta etapa demuestra el nivel de riesgo real al que está expuesta la organización (CEH v11, s. f.).

Herramienta ejemplo: Metasploit, plataforma robusta para la ejecución de exploits y pruebas de acceso.

Escalada De Privilegios, Persistencia Y Movimientos Laterales

Después del acceso inicial, se busca mantener el control del sistema, escalar privilegios y moverse lateralmente dentro de la red, simulando un atacante avanzado (Herzog, 2010).

Herramienta ejemplo: Mimikatz, utilizada para obtener credenciales y realizar elevación de privilegios en sistemas Windows.

Informe De Resultados

Finalmente, se genera un informe detallado con los hallazgos, vulnerabilidades detectadas, riesgos asociados y recomendaciones para mitigar cada falla. Este informe debe ser claro, técnico y accionable (CSIRT Académico UNAD, s. f.).

Herramienta ejemplo: Dradis Framework, diseñada para organizar y presentar los resultados de forma profesional.

Las Herramientas De Ciberseguridad

En el ámbito de la ciberseguridad, especialmente en escenarios de evaluación ofensiva como las pruebas de penetración (pentesting), existe un conjunto diverso de herramientas que permiten identificar vulnerabilidades, simular ataques y evaluar la seguridad de infraestructuras tecnológicas.

A continuación, se describen algunas de las herramientas más utilizadas por profesionales del Red Team y analistas de seguridad ofensiva, junto con recursos en línea clave para el reconocimiento y análisis de vulnerabilidades.

Metasploit Framework

Metasploit es una plataforma de código abierto desarrollada por la empresa Rapid7, ampliamente reconocida en el ámbito del hacking ético y las pruebas de penetración. Su diseño modular permite realizar simulaciones de ataques cibernéticos de manera controlada, aprovechando vulnerabilidades documentadas en múltiples sistemas operativos, aplicaciones y dispositivos.

Metasploit integra componentes reutilizables como exploits (código que aprovecha una falla), payloads (cargas útiles que ejecutan comandos una vez comprometido el sistema), encoders (para evadir detección por antivirus) y herramientas auxiliares que facilitan procesos de escaneo, evasión, persistencia y post-explotación. Es una herramienta clave en la formación y práctica de analistas de seguridad ofensiva (Rapid7, s. f.).

Nmap (Network Mapper)

Nmap, desarrollado por Gordon Lyon (alias Fyodor), es una herramienta esencial para el escaneo y mapeo de redes. Su principal función es identificar dispositivos activos en una red, detectar puertos abiertos y reconocer los servicios que se están ejecutando.

Lo que distingue a Nmap es su potente motor de scripting, Nmap Scripting Engine (NSE), que permite realizar auditorías más profundas al automatizar tareas como la detección de vulnerabilidades, el reconocimiento de versiones de software y la ejecución de pruebas personalizadas. Nmap es ampliamente utilizado en las etapas iniciales de reconocimiento dentro del ciclo de pruebas de penetración (Nmap.org, s. f.).

OpenVAS (Open Vulnerability Assessment System)

OpenVAS es una solución de escaneo de vulnerabilidades de código abierto desarrollada y mantenida por Greenbone Networks. Su propósito es identificar debilidades de seguridad en infraestructuras de red mediante análisis automatizados.

Este sistema emplea una base de datos constantemente actualizada con vulnerabilidades conocidas (incluyendo CVEs), lo que permite evaluar la exposición de servidores, servicios y dispositivos ante amenazas específicas. Es especialmente útil en auditorías de cumplimiento y revisiones periódicas de seguridad dentro de entornos empresariales (Greenbone, s. f.).

Servicios En Línea Para La Identificación De Vulnerabilidades

Exploit Database (ExploitDB)

ExploitDB es una plataforma pública administrada por Offensive Security que funciona como un repositorio de exploits, scripts de prueba y demostraciones de vulnerabilidades (proof of concept – PoC).Este recurso es alimentado por la comunidad global de investigadores en seguridad y sirve como una referencia técnica indispensable para identificar, analizar y reproducir vulnerabilidades conocidas en aplicaciones, sistemas operativos y hardware.

Durante las fases de análisis y explotación en pruebas de penetración, los profesionales consultan ExploitDB para verificar si existen vectores de ataque documentados que puedan aplicarse al entorno objetivo (Offensive Security, s. f.).

Common Vulnerabilities and Exposures (CVE)

CVE es un sistema estandarizado gestionado por la corporación MITRE, cuyo objetivo es catalogar de forma precisa las vulnerabilidades de seguridad en software y hardware. Cada vulnerabilidad registrada recibe un identificador único (por ejemplo, CVE-2024-XXXX), lo que facilita su rastreo, comparación y análisis por parte de la comunidad de ciberseguridad.

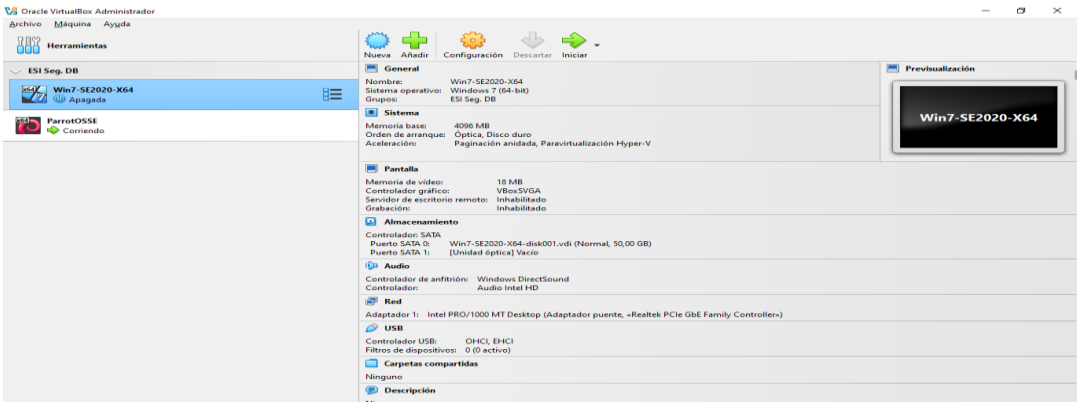
Numerosas herramientas de escaneo y evaluación de vulnerabilidades, como OpenVAS y Nessus, utilizan las entradas de CVE para estructurar sus análisis. La base de datos CVE se ha convertido en un estándar de referencia internacional para la gestión de vulnerabilidades en entornos corporativos y gubernamentales (MITRE, s. f.).

Banco De Trabajo

A. Herramienta “VirtualBox”

Figura 1

Herramienta VirtualBox

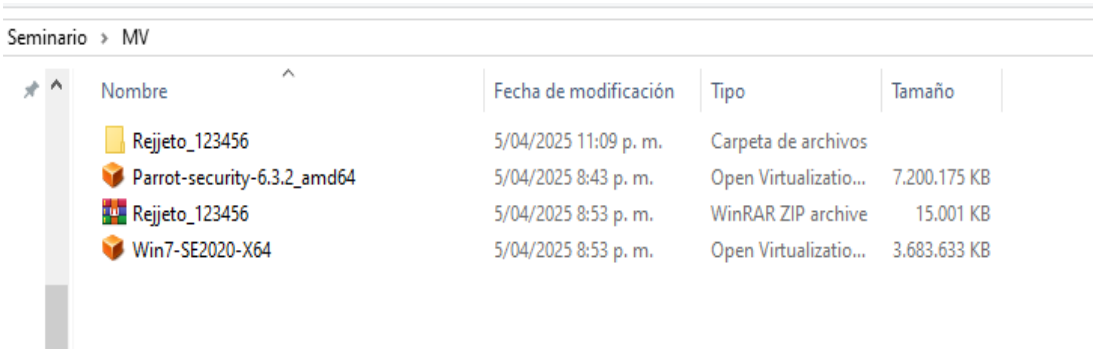


Fuente, Elaboración Propia

B. Importación de las imágenes en formato OVA de los sistemas operativo Windows y Linux

Figura 2

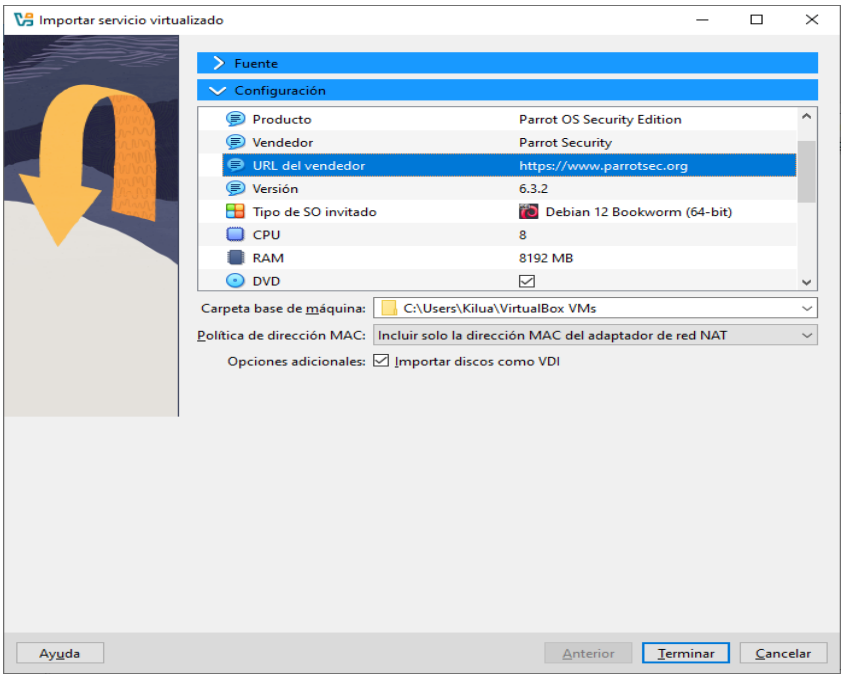
Imágenes a ova para importar a VirtualBox



Fuente, Elaboración Propia

Figura 3

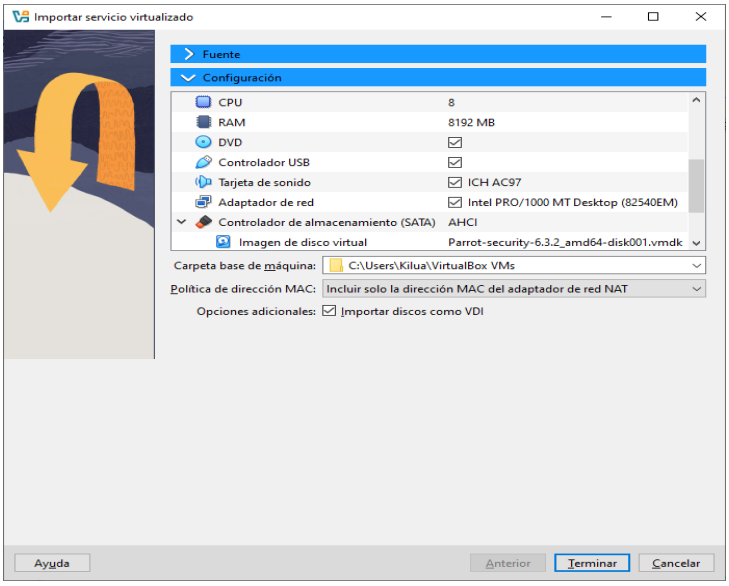
Menú de importación de Linux



Fuente, Elaboración Propia

Figura 4

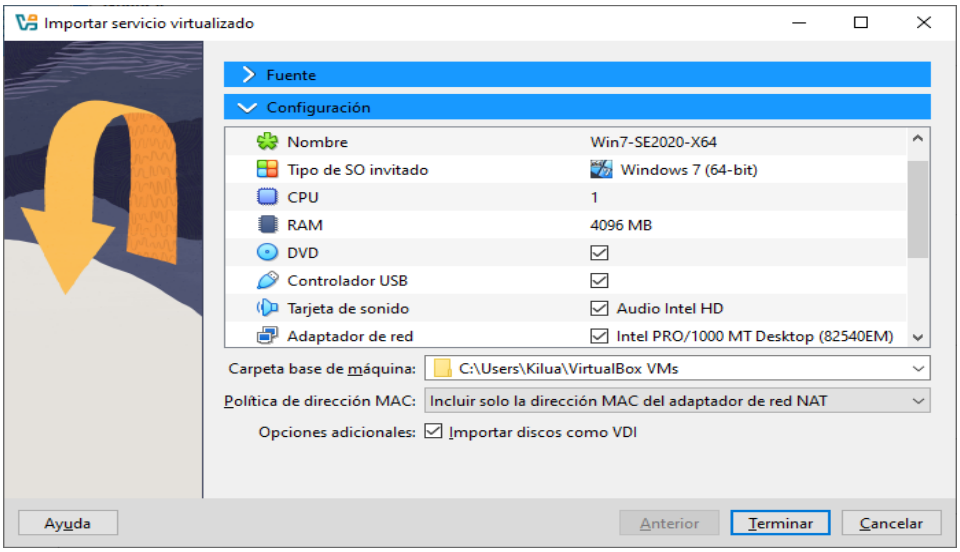
Menú de configuración de importación Linux



Fuente, Elaboración Propia

Figura 5

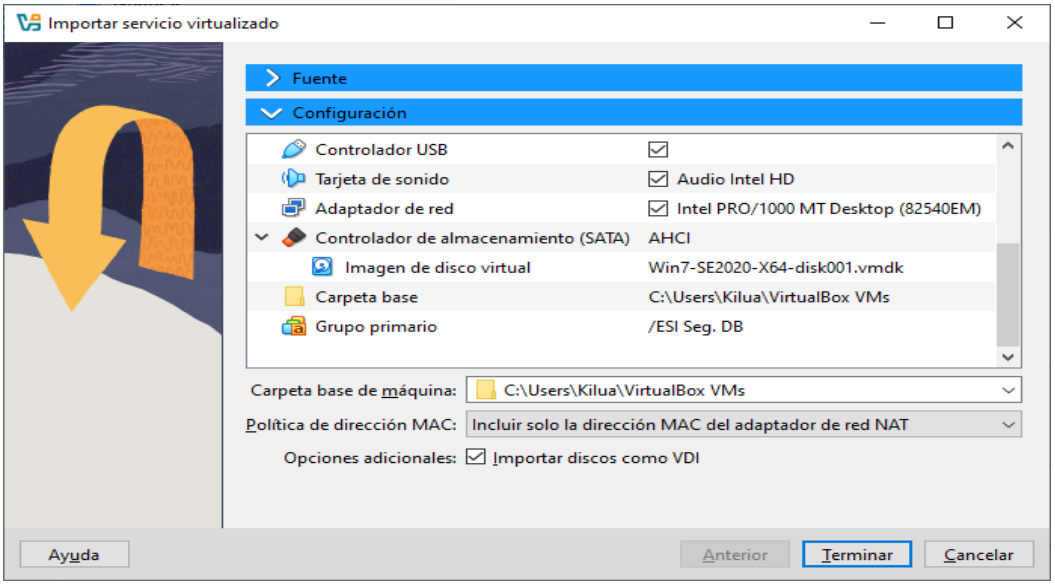
Menú de importación de Windows



Fuente, Elaboración Propia

Figura 6

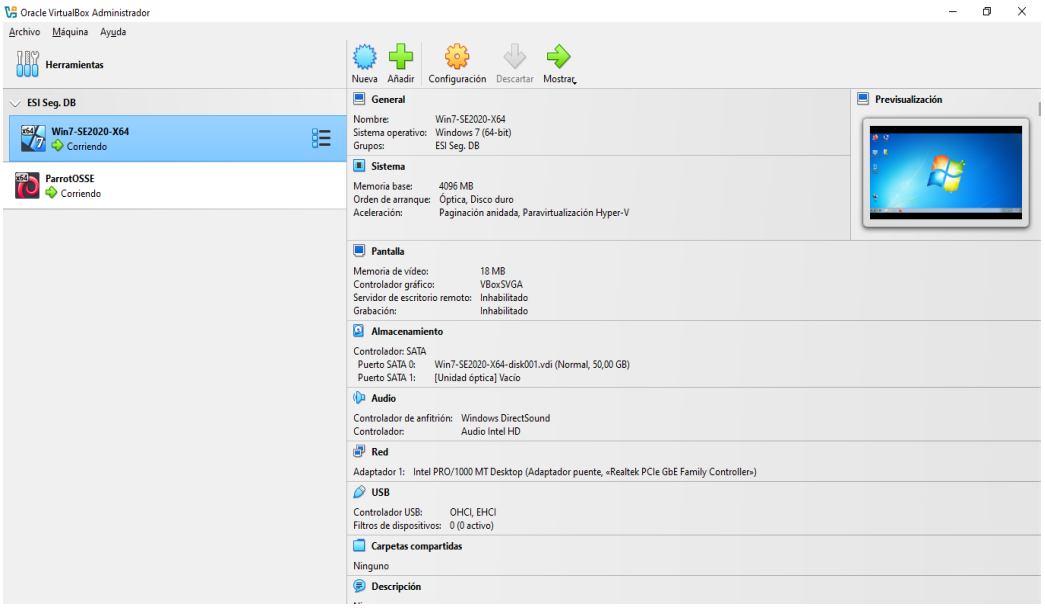
Menú de configuración de importación de Linux



Fuente, Elaboración Propia

Figura 7

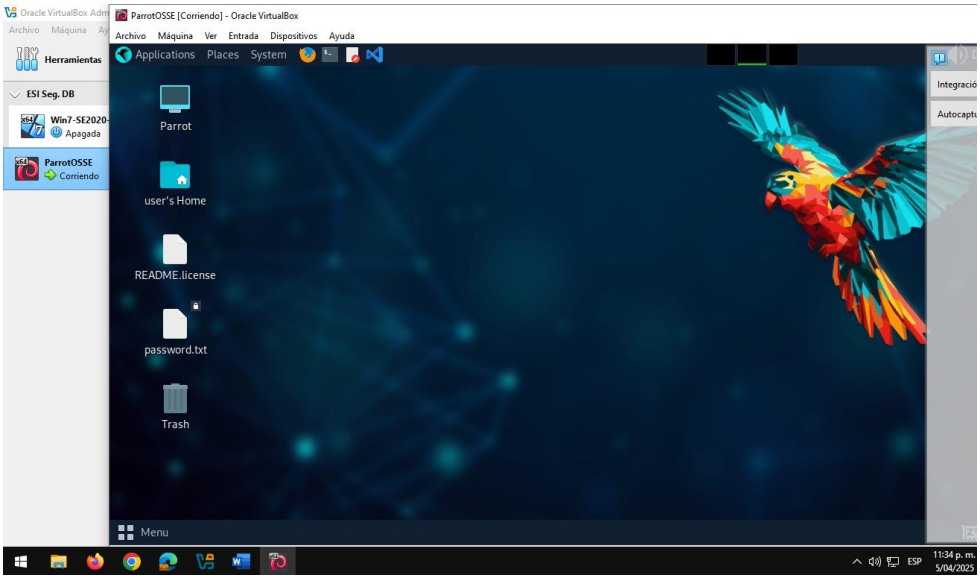
Máquinas virtuales corriendo



Fuente, Elaboración Propia

Figura 8

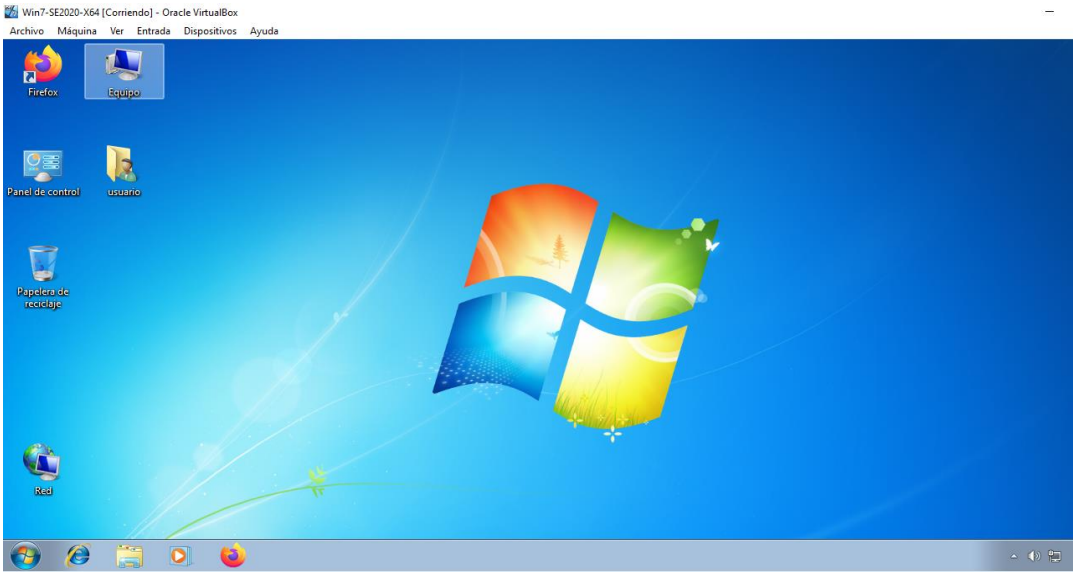
Evidencia operación correcta de Linux



Fuente, Elaboración Propia

Figura 9

Evidencia operación máquina de Windows

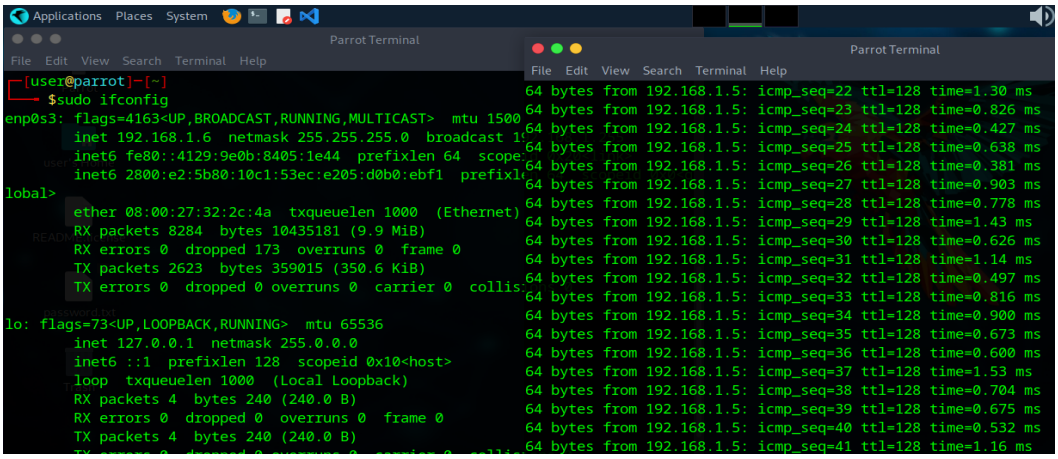


Fuente, Elaboración Propia

C. Comunicación entre las máquinas virtuales

Figura 10

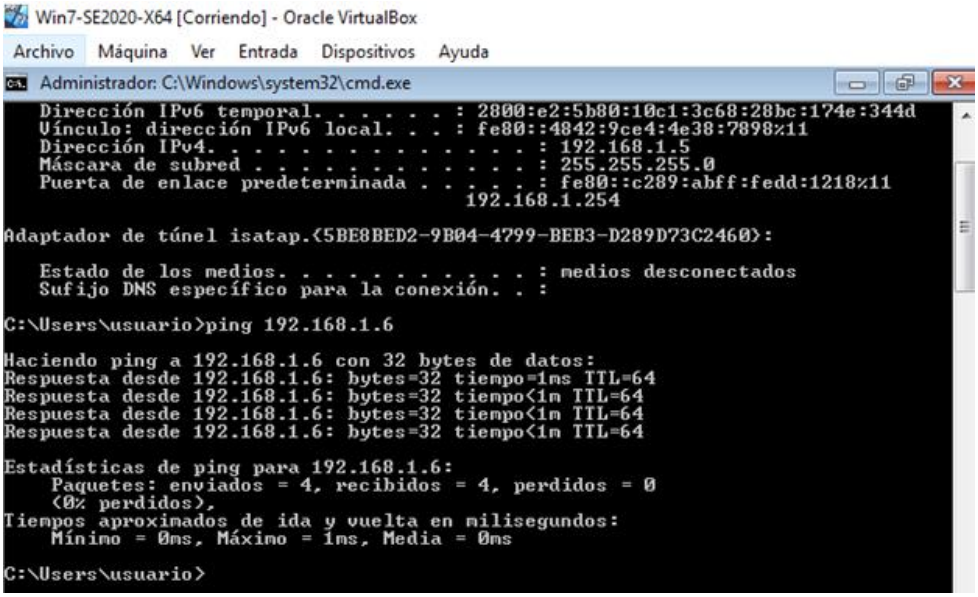
Prueba de conectividad de Linux hacia Windows



Fuente, Elaboración Propia

Figura 11

Prueba de conectividad de Windows hacia Linux

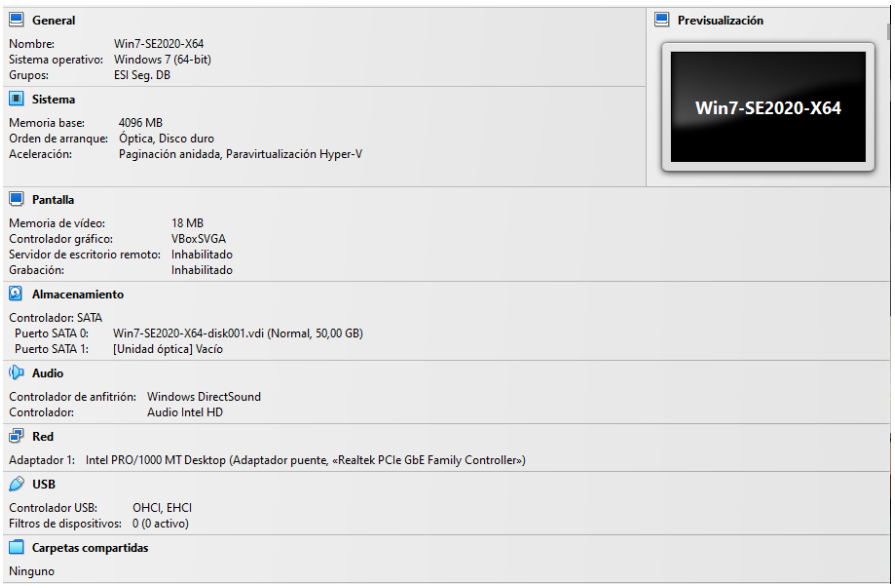


Fuente, Elaboración Propia

D. Características técnicas de hardware

Figura 12

Características técnicas Windows

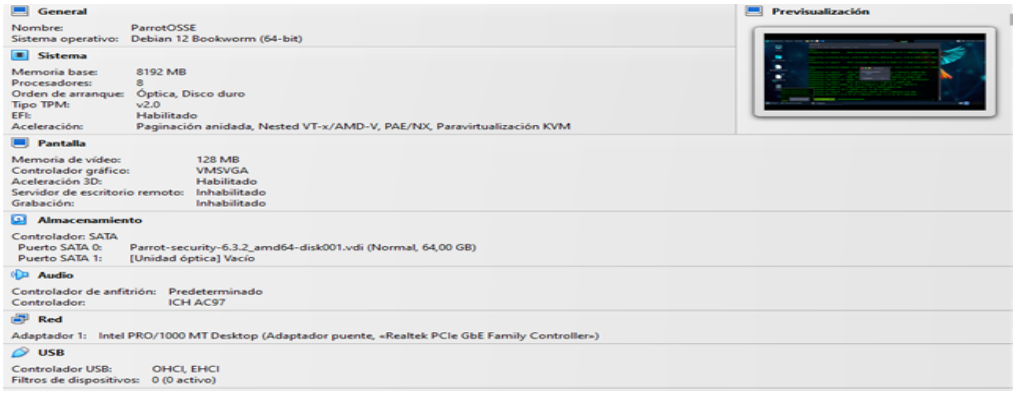


Fuente, Elaboración Propia

Windows 7 funciona con 4 GB de RAM, cantidad suficiente para ejecutar tareas básicas como el uso de software de oficina, navegación web y aplicaciones livianas. Al igual que el sistema anterior, puede estar desplegado en una máquina física o virtual, y el adaptador en puente le permite obtener su propia dirección IP dentro de la red, facilitando la interacción con otros dispositivos sin necesidad de pasar por una red compartida o enmascarada (NAT).

Figura 13

Características técnicas de Linux



Fuente, Elaboración Propia

Parrot OS, al estar basado en Linux, hace un uso eficiente de los recursos asignados. Los 8 GB de RAM permiten ejecutar de manera fluida diversas herramientas orientadas a la seguridad informática, análisis forense y pruebas de penetración. Este sistema puede estar instalado en una máquina física o virtual, y gracias al adaptador en modo puente, se conecta directamente a la red local. Esto le permite obtener una dirección IP propia y comunicarse con otros dispositivos de la red como si fuera un equipo independiente.

En esta configuración se ha desplegado un sistema operativo Parrot OS basado en Linux, al que se le han asignado 8 GB de memoria RAM, y un sistema Windows 7 con 4 GB de RAM. Ambos cuentan con un adaptador de red configurado en modo puente.

El uso del adaptador en modo puente es fundamental en este tipo de despliegue, ya que permite que ambos sistemas operativos se integren a la red como si fueran equipos físicos reales, lo cual es especialmente útil para pruebas de red, transferencia de archivos, y simulaciones en entornos reales.

Etapa 2 Actuación Ética Y Legal

Identificar Cualquier Procedimiento Ilegal O Poco Ético Que Se Esté Contemplando En El Acuerdo Mencionado

Considero que La situación planteada en la organización CyberFort Technologies se evidencia una serie de irregularidades legales y éticas que deben solventadas de acuerdo con las normas legales colombianas.

En primer lugar, el hecho de que los contratos hayan sido elaborados por un abogado desvinculado de la empresa por posibles actos ilícitos, y que estos no hayan sido revisados por la gerencia actual, genera dudas sobre su validez jurídica, lo cual vulnera el principio de buena fe contractual consagrado en el artículo 1602 del Código Civil y va en contra de las obligaciones profesionales contempladas en la Ley 1123 de 2007.

En segundo lugar, asignar tareas técnicas como parte de una "prueba de admisión", sin haber firmado previamente un contrato, podría configurarse como una relación laboral encubierta, infringiendo el artículo 23 del Código Sustantivo del Trabajo, que establece los elementos esenciales de una relación laboral, y el artículo 25 de la Constitución Política, que protege el derecho a un trabajo digno.

En tercer lugar, la entrega de acuerdos de confidencialidad sin revisión legal previa ni consentimiento informado podría vulnerar lo establecido en la Ley 1581 de 2012 sobre protección de datos personales, especialmente los principios de legalidad, finalidad, proporcionalidad y libertad.

En cuarto lugar, el desarrollo de pruebas técnicas sin autorización clara, especialmente si implican actividades propias de los equipos Red Team o Blue Team como análisis de vulnerabilidades, escaneos o simulaciones de intrusión, podría contravenir lo establecido en la Ley 1273 de 2009, que penaliza conductas como el acceso no autorizado a sistemas informáticos, la interceptación de datos y el uso indebido de información personal.

En consecuencia, que se revisen y actualicen los contratos y acuerdos bajo supervisión jurídica, se delimiten claramente las responsabilidades técnicas autorizadas y se garantice la protección de los derechos laborales y personales de quienes participan en el proceso de selección.

Señalar Qué Artículos De La Ley 1273 Podrían Ser Infringidos En El Acuerdo Y Detallar Las Razones Por Las Cuales Dichos Artículos Serían Vulnerados

El acuerdo incluye cláusulas que podrían inducir a los firmantes a ocultar información ilegal, restringir el derecho a denunciar delitos informáticos y encubrir conductas ilícitas bajo el pretexto de la confidencialidad. Esto podría vulnerar varios artículos de la Ley 1273 de 2009, La cual establece como delitos diversas conductas vinculadas a la protección de la información y los datos, los cuales detallo a continuación:

Artículo 269A – Ingreso no autorizado y uso indebido de un sistema informático

Razón de vulneración. El contrato menciona que la información relacionada con las actividades internas de ciberseguridad debe mantenerse confidencial, pero prohíbe la divulgación o denuncia de accesos no autorizados. Esto podría ocultar acciones de acceso ilegal a sistemas informáticos, lo que contraviene este artículo de la ley, que sanciona el acceso no autorizado.

Artículo 269C – Captura No Autorizada De Información Digital Durante Su Transmisión O Almacenamiento

Razón de vulneración. En el contrato se menciona que la información relacionada con "chuzadas" e interceptaciones de información es confidencial. Esto sugiere que las interceptaciones ilegales de datos podrían ser tratadas como información protegida, lo que contraviene este artículo, que tipifica la interceptación no autorizada de datos.

Artículo 269E – Infracción O Acceso No Autorizado A Información Personal

Razón de vulneración. El contrato prohíbe denunciar el manejo indebido de información, incluyendo datos personales. Esto podría dar lugar al almacenamiento o uso de datos personales sin el debido consentimiento, vulnerando el derecho a la privacidad de los individuos, conforme a lo estipulado por este artículo.

Artículo 269F – Uso De Software Malicioso

Razón de vulneración. Si el equipo Red Team utiliza herramientas como malware, troyanos o software de espionaje sin la debida autorización legal y supervisión, estas acciones estarían tipificadas como uso de software malicioso. El contrato, al proteger la confidencialidad de dichas prácticas, podría estar encubriendo una actividad ilegal, lo cual contraviene este artículo.

Artículo 269I – Violación De Medidas Tecnológicas

Razón de vulneración. Durante las pruebas o simulaciones, si el equipo elude medidas de protección tecnológica (como contraseñas, encriptación o licencias digitales) sin una autorización formal y legal correspondiente, se podría estar vulnerando este artículo.

El contrato no establece límites claros para estas acciones, lo que genera un riesgo jurídico de violar las medidas tecnológicas de protección.

Artículo 269D – Daño Informático (Posible Vulneración)

Razón de vulneración. Si, durante las actividades de prueba o simulación, se altera, borra o daña información sin la debida autorización —incluso si se realiza como parte de un ataque simulado— y esta conducta es protegida por las cláusulas de confidencialidad, se podría estar encubriendo un delito de daño informático.

Justificar Respuesta, Ya Sea En Apoyo O En Contra, Y Tener En Cuenta En La Justificación Que Dispone De Una Copia Del Código De Ética Correspondiente A La Profesión De Ingeniería

Como experto en ciberseguridad, no aceptaría este trabajo, A continuación, explico las razones detrás de mi decisión, tomando en cuenta tanto los procesos poco confiables del acuerdo al Código de Ética

Confusión Sobre La Ética Profesional

El contrato de confidencialidad propuesto plantea riesgos éticos y legales significativos, como la obligación de no denunciar actividades sospechosas o ilegales relacionadas con el acceso no autorizado a sistemas informáticos. Como profesional de la ciberseguridad, mi principal responsabilidad es proteger la información, la infraestructura tecnológica y la privacidad de las personas y organizaciones, conforme a principios éticos. Encubrir o no poder denunciar conductas ilícitas va en contra de estos principios y no está alineado con los estándares éticos que debo seguir.

Impacto Negativo En La Reputación Profesional

Trabajar en un entorno donde se permiten o se encubren prácticas ilegales podría afectar seriamente mi reputación profesional. La ética en ciberseguridad es crucial, y asociarme con una organización que no respeta estos principios podría tener consecuencias duraderas en mi carrera.

Posible Vulneración De La Ley

Las cláusulas del contrato podrían contravenir la Ley 1273 de 2009, que tipifica delitos como el acceso no autorizado a sistemas informáticos, la interceptación ilegal de datos y el uso de software malicioso. Como ingeniero en ciberseguridad, debo asegurarme de que todas las actividades que realice sean legales y éticas. El contrato podría incitar a realizar actividades ilícitas, lo que comprometería la seguridad y la integridad de la información.

Cumplimiento Del Código De Ética De La COPNIA

El Código de Ética de la COPNIA establece que se debe actuar con honestidad, imparcialidad y responsabilidad en su trabajo. Entre los principios que resalta están:

Confianza pública. Debemos proteger la integridad de la información y no involucrarnos en prácticas que puedan dañar la confianza pública.

Cumplimiento de la ley. Los ingenieros deben respetar siempre la legislación vigente. El contrato propuesto parece promover actividades que podrían violar las leyes colombianas, como la Ley 1273 de 2009.

Evitar conflictos de interés. Si me uniera a una organización con cláusulas contractuales que pudieran ponerme en una situación ética comprometida, estaría violando el principio de imparcialidad y actuando en contra de mis responsabilidades profesionales.

Responsabilidad Frente A Terceros

Como experto en ciberseguridad, también tengo la responsabilidad de proteger a los terceros que pudieran verse perjudicados por las decisiones de la entidad. El contrato de confidencialidad podría llevarme a participar en actividades que perjudican a otras personas o empresas, sin posibilidad de denuncia o defensa.

Aunque el salario y el contrato son atractivos, no aceptaría este puesto debido a los problemas éticos y legales evidentes en el acuerdo, que comprometen mis principios profesionales y mi responsabilidad como ingeniero en ciberseguridad.

¿Qué Nivel De Acceso Deben Tener Las Empresas De Ciberseguridad A La Información Confidencial De Sus Clientes Durante Una Auditoría De Seguridad, Y De Qué Manera Se Puede Asegurar Que Este Acceso No Sea Utilizado De Forma Inapropiada?

Durante una auditoría de seguridad, es fundamental que se cuenten con un acceso regulado a información sensible, con el propósito de identificar amenazas, vulnerabilidades y posibles brechas. Sin embargo, este acceso debe estar claramente delimitado mediante acuerdos contractuales que definan el alcance de la auditoría, los límites del uso de la información y las responsabilidades del personal involucrado.

Este acceso debe ser proporcional, temporal y restringido exclusivamente a los fines técnicos y operativos de la evaluación. En el contexto colombiano, estos procesos deben alinearse con la Ley 1581 de 2012, que regula la protección de datos personales, y con la Ley 1273 de 2009, que penaliza el acceso abusivo a sistemas informáticos y el uso indebido de información confidencial.

¿Qué Medidas De Supervisión Y Control Deben Establecerse En Las Empresas De Ciberseguridad Para Prevenir Que Sus Empleados Utilicen Herramientas Avanzadas De Análisis Forense Con Fines No Autorizados O Éticamente Problemáticos?

Se deben contar con mecanismos de control interno sólidos que supervisen de manera continua las actividades del personal técnico, especialmente cuando manejan herramientas avanzadas de análisis forense digital.

Estos mecanismos incluyen controles de acceso diferenciados, temporales y ajustados al rol del usuario; auditorías internas periódicas que verifiquen el cumplimiento de protocolos; capacitaciones constantes sobre ética profesional y uso responsable de la información; así como la implementación de canales de denuncia confidenciales para reportar posibles irregularidades. Además, es indispensable que los contratos laborales y los códigos internos de ética incluyan cláusulas claras sobre sanciones en caso de uso indebido de la información. Estas acciones se alinean con las disposiciones del artículo 269F del Código Penal Colombiano y con los principios éticos establecidos por el COPNIA para el ejercicio profesional de la ingeniería.

¿Cómo Deberían Actuar Los Gobiernos Y Las Organizaciones Al Descubrir Que Una Empresa De Ciberseguridad Contratada Ha Llevado A Cabo Actividades De Ciber Espionaje?

Ante casos comprobados de ciber espionaje cometidos por empresas contratadas, los gobiernos y organizaciones deben actuar con firmeza y transparencia. En primer lugar, deben denunciar penalmente los hechos ante las autoridades judiciales, con base en la Ley 1273 de 2009, que sanciona delitos informáticos como el acceso no autorizado, la interceptación de datos y la violación de información confidencial.

De manera paralela, se debe cancelar inmediatamente el contrato con la empresa involucrada y abrir una investigación administrativa. También es necesario exigir compensaciones por los daños causados, tanto materiales como reputacionales, e informar a otras entidades del sector público o privado para prevenir futuros incidentes similares. Estas medidas garantizan la protección institucional, refuerzan la legalidad en la contratación y promueven la rendición de cuentas.

¿Qué Acciones Serían Apropiadas Para Recuperar La Confianza Y Garantizar Que No Se Repita La Situación?

Para recuperar la confianza institucional es fundamental elevar los estándares de contratación pública y privada. Esto implica incluir cláusulas más estrictas sobre el manejo de información sensible, responsabilidades legales, auditoría y sanciones. También se recomienda exigir certificaciones internacionales como la norma ISO/IEC 27001, o el cumplimiento de lineamientos nacionales como el Esquema de Ciberseguridad del MinTIC.

Etapa 3 Ejecución Pruebas De Intrusión

Conjunto De Herramientas De Software Empleadas En Las Pruebas De Penetración Realizadas Y Evidencia De Los Comandos Utilizados Incluyendo Resultados

Para llevar a cabo la identificación de vulnerabilidades en la máquina objetivo, se empleará la herramienta Nmap, la cual permitirá realizar un escaneo detallado de los puertos abiertos, servicios en ejecución y versiones de software expuestas. Esta información es clave para detectar posibles vectores de ataque.

Posteriormente, se utilizará el framework Metasploit, una plataforma robusta para la explotación de vulnerabilidades, con el fin de validar si alguno de los servicios detectados es susceptible a ataques conocidos. A través de Metasploit se procederá con la carga del exploit correspondiente, permitiendo ejecutar código malicioso en el sistema comprometido o alcanzar una Shell remota.

Este procedimiento tiene como objetivo simular un ataque real, evaluar el nivel de exposición del sistema y comprobar si es posible una escalación de privilegios o el acceso no autorizado con fines de análisis técnico a través de la metodología red team.

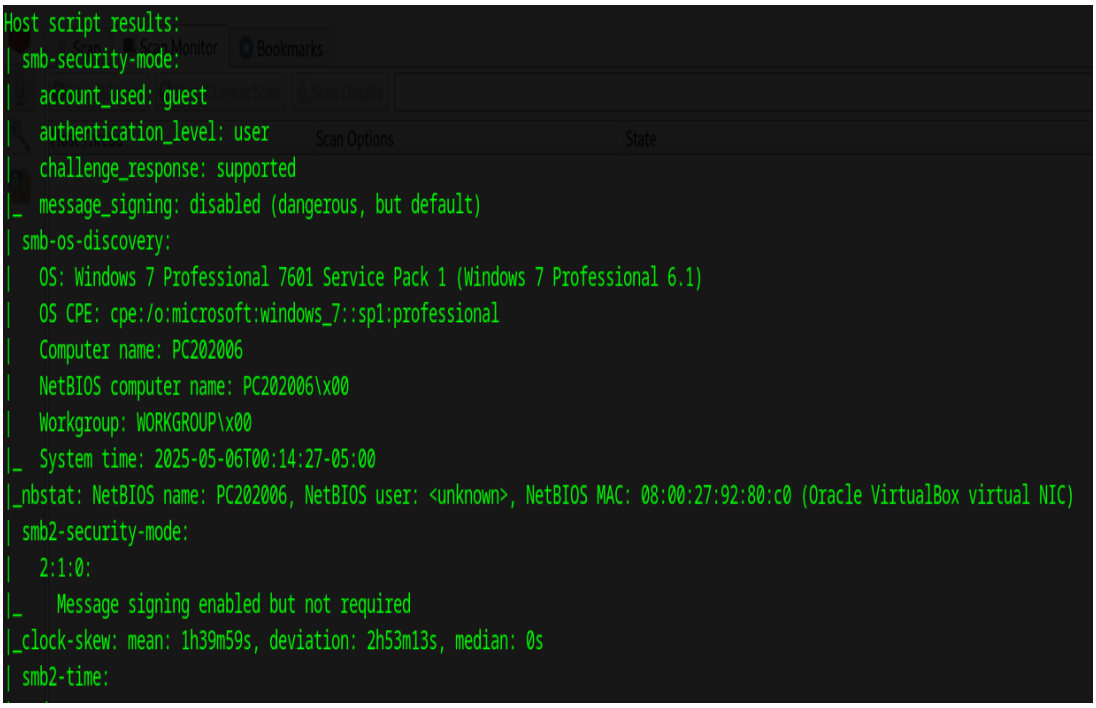
Herramienta NMAP

Para iniciar el reconocimiento del equipo objetivo, se utiliza el comando nmap -A 192.168.2.101, el cual permite realizar un escaneo avanzado sobre la dirección IP especificada. La opción -A habilita funciones clave como la detección del sistema operativo, la identificación de versiones de servicios activos, la ejecución de scripts del motor NSE (Nmap Scripting Engine) y un traceroute para analizar la ruta hacia el host.

Esta combinación de técnicas proporciona información detallada sobre la superficie de ataque del sistema, permitiendo identificar posibles vulnerabilidades y facilitando la selección de herramientas o exploits adecuados para una posterior fase de prueba de penetración**.**

Figura 14

Detección de sistema operativo

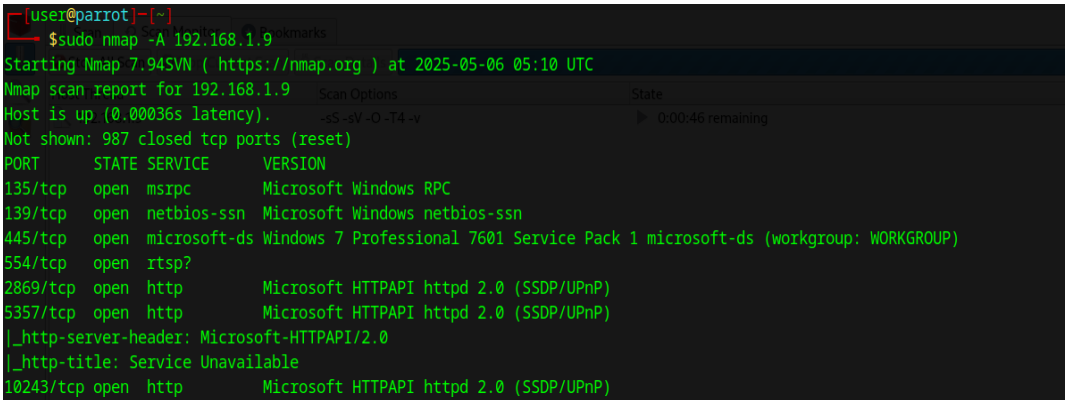


Fuente, Elaboración Propia

Durante la fase de reconocimiento, se ejecutó un escaneo con el comando nmap -A 192.168.2.101, lo que permitió identificar información relevante sobre el sistema objetivo. Entre los resultados obtenidos, se detectó que el equipo estaba ejecutando Microsoft Windows 7, lo cual fue determinado a través de la función de detección de sistema operativo integrada en Nmap.

Figura 15

Ejecución de comando nmap -A

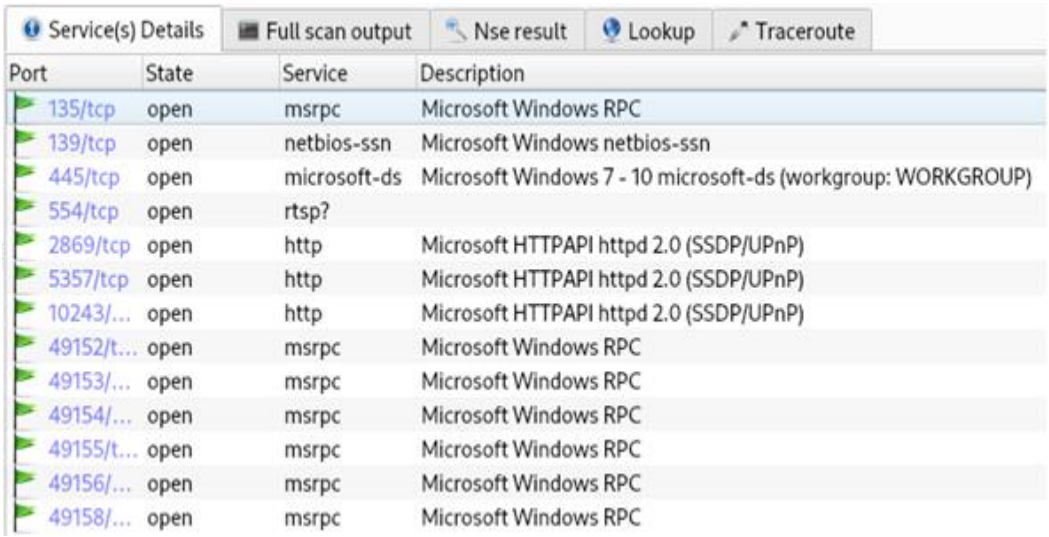


Fuente, Elaboración Propia

Durante el escaneo realizado con el comando nmap -A 192.168.2.101, se identificaron varios puertos abiertos en el sistema objetivo, lo que permitió obtener una visión más clara de los servicios expuestos.

Figura 16

Puertos abiertos durante nmap



Fuente, Elaboración Propia

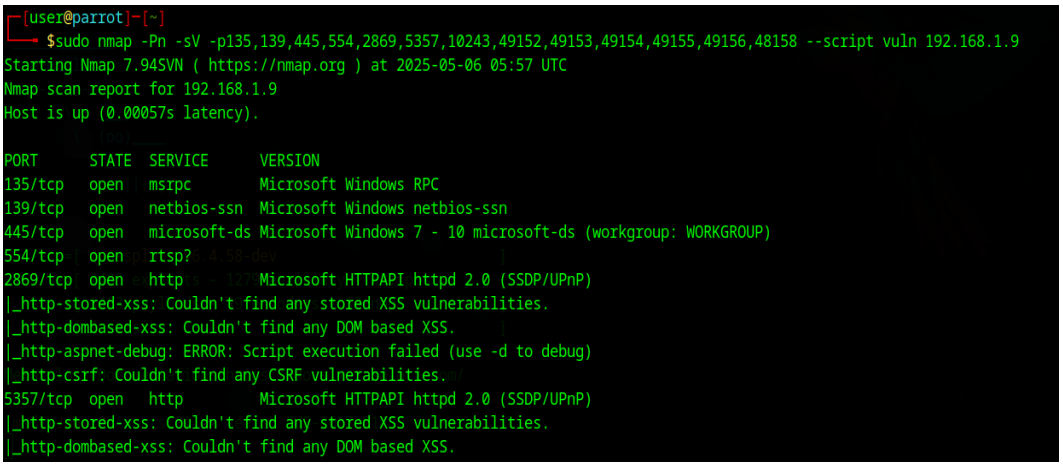
Ahora que hemos encontrado una selección de puertos comúnmente utilizados en sistemas Windows como SMB (135, 139, 445), servicios de transmisión (554), y servicios del sistema operativo como WS-Discovery y DCOM los cuales usaremos para realizar el ataque.

Usaremos el siguiente comando para realizar un escaneo detallado de vulnerabilidades en servicios específicos de un host, en este caso la IP 192.168.1.9 sudo nmap -Pn -sV -p135,139,445,554,2869,5357,10243,49152,49153,49154,49155,49156,48158 --script vuln 192.168.1.9. La opción -Pn omite el ping inicial, asumiendo que el host está activo, lo cual es útil cuando existen restricciones de red que bloquean ICMP. El parámetro -sV permite identificar las versiones de los servicios que se encuentran activos en los puertos definidos con -p.

Además, la opción --script vuln activa el motor de scripts de Nmap (NSE) enfocado en la detección de vulnerabilidades conocidas, permitiendo identificar posibles fallos de seguridad en los servicios expuestos. Este comando es clave en la fase de enumeración de un pentest, ya que facilita la recolección de información precisa para evaluar el riesgo de cada servicio y planificar posibles vectores de ataque.

Figura 17

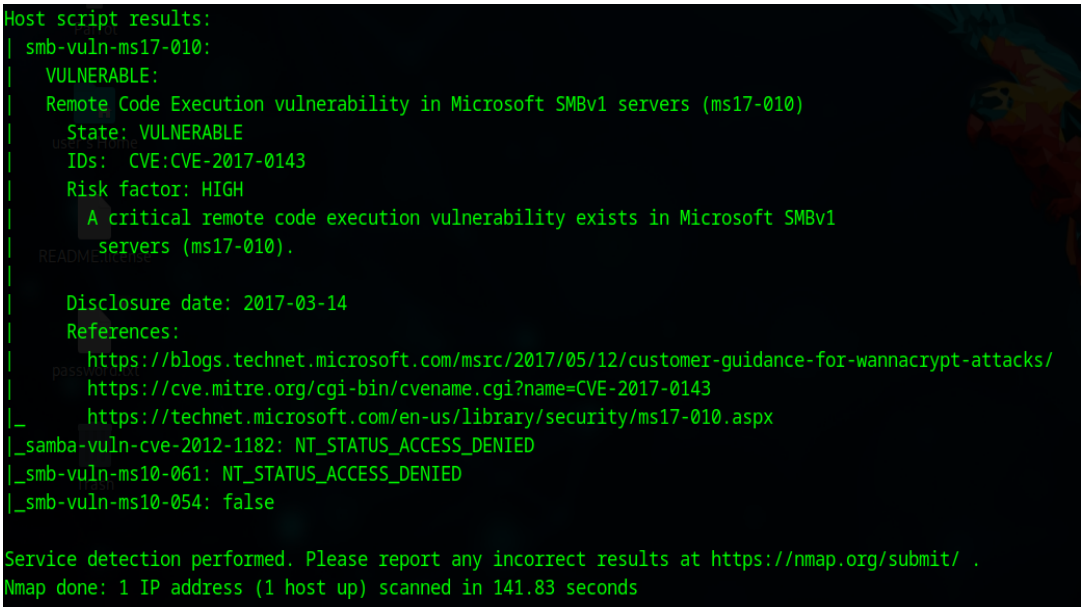
Ejecución de comandos y puertos vulnerables



Fuente, Elaboración Propia

Figura 18

Vulnerabilidad identificada



Fuente, Elaboración Propia

Hemos identificado La vulnerabilidad CVE-2017-0143 la cual es una vulnerabilidad crítica descubierta en el protocolo SMBv1 (Server Message Block versión 1) de Microsoft Windows. Esta falla, que forma parte del conjunto de vulnerabilidades conocido como "EternalBlue", la vulnerabilidad permite la ejecución remota de código (RCE) sin autenticación, mediante el envío de paquetes especialmente diseñados al puerto 445/TCP, utilizado por el servicio SMB. Esta falla afecta múltiples versiones de Windows, incluyendo Windows XP, 7, 8, Server 2003 y 2008, especialmente si SMBv1 está habilitado

Herramienta Metasploit Framework

Para buscar y explotar la vulnerabilidad CVE-2017-0143 en Metasploit Framework, primero debes iniciar Metasploit con el comando Msfconsole. Usaremos buscar el exploit correspondiente utilizando Search cve-2017-0143

Figura 19

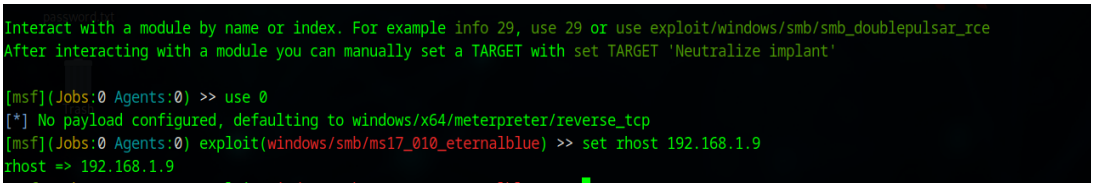
Ejecución comando search cve-2017-0143

Fuente, Elaboración Propia

Esto cargará el módulo de explotación para la vulnerabilidad EternalBlue, permitiéndote configurarlo y ejecutarlo según las necesidades de tu prueba de penetración. El comando use es fundamental para navegar entre los diferentes módulos disponibles en Metasploit y activar las funcionalidades necesarias para un ataque controlado, Usaremos el comando use se emplea para seleccionar un módulo específico que se desea utilizar. Este comando permite acceder a distintos tipos de módulos donde utilizaremos el 0

Figura 20

Ejecución de comando use 0 y rhosts

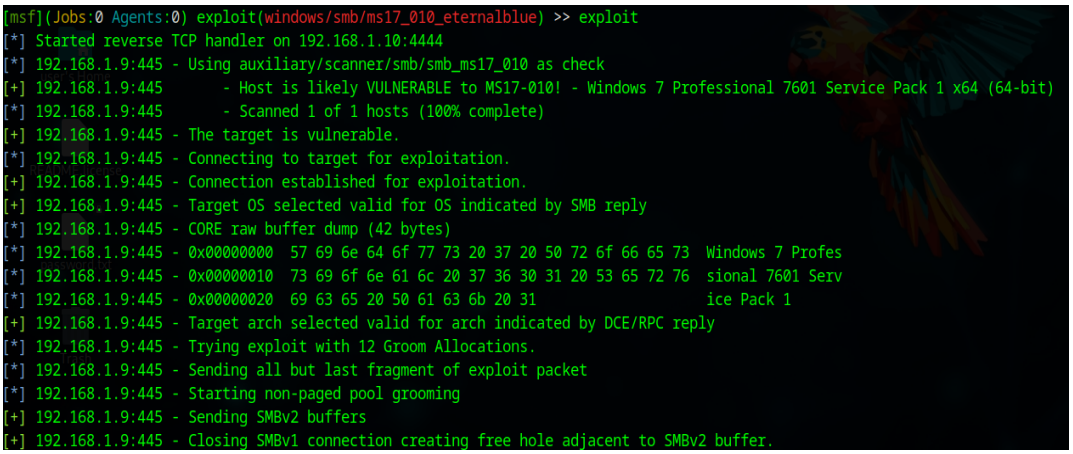


Fuente, Elaboración Propia

Configuraremos las opciones necesarias, como la dirección IP del objetivo (RHOSTS) y Para configurar la IP del objetivo posteriormente seleccionado el objetivo ejecutaremos el exploit

Figura 21

Ejecución de exploit



Fuente, Elaboración Propia

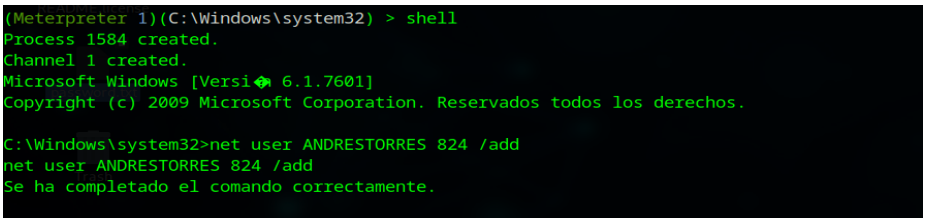
Al ejecutar el exploit no cargara Meterpreter es un payload avanzado utilizado en Metasploit Framework, que permite a los atacantes obtener acceso remoto a una máquina comprometida y ejecutar una amplia variedad de acciones sin necesidad de interactuar directamente con el sistema operativo víctima.

A diferencia de otros payloads, Meterpreter no deja rastros visibles en el sistema objetivo, ya que se ejecuta en la memoria y no en el disco, lo que dificulta su detección.

Usaremos comando shell la cual es una funcionalidad que permite al atacante obtener acceso a una shell interactiva en el sistema comprometido este comando proporciona una interfaz de línea de comandos directa en el sistema de la víctima, lo que permite ejecutar comandos del sistema operativo de manera convencional.

Figura 22

Ejecución de meterpreter



Fuente, Elaboración Propia

Ahora usaremos Los comandos net user ANDRESTORRES 824 /add y net localgroup Administradores ANDRESTORRES /add son utilizados en sistemas Windows para gestionar usuarios y grupos.

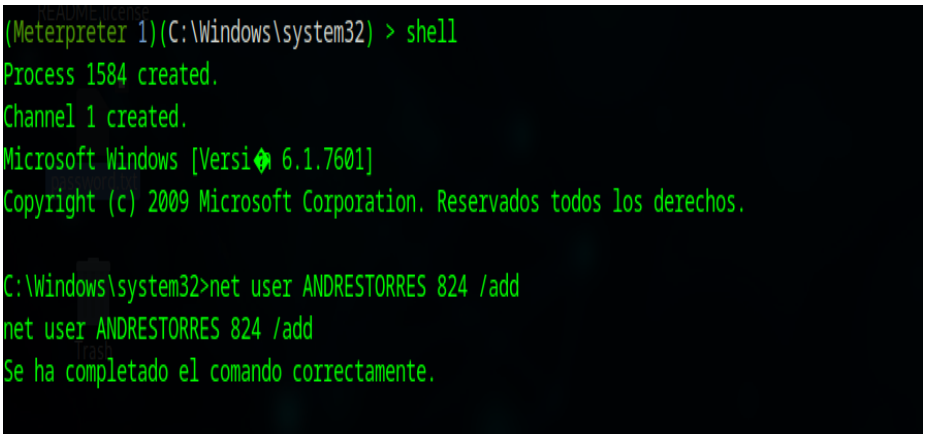
El primer comando, net user ANDRESTORRES 824 /add, crea un nuevo usuario llamado ANDRESTORRES con la contraseña 824 en el sistema. Este comando es útil cuando se desea agregar un usuario nuevo sin privilegios específicos.

El segundo comando, net localgroup Administradores ANDRESTORRES /add, agrega el usuario ANDRESTORRES al grupo Administradores, lo que le concede privilegios elevados y control total sobre el sistema, permitiéndole realizar cambios significativos, acceder a archivos protegidos y ejecutar comandos de administrador.

También ejecutaremos el comando net users es una herramienta de línea de comandos en Windows que permite gestionar y ver las cuentas de usuario en un sistema.

Figura 23

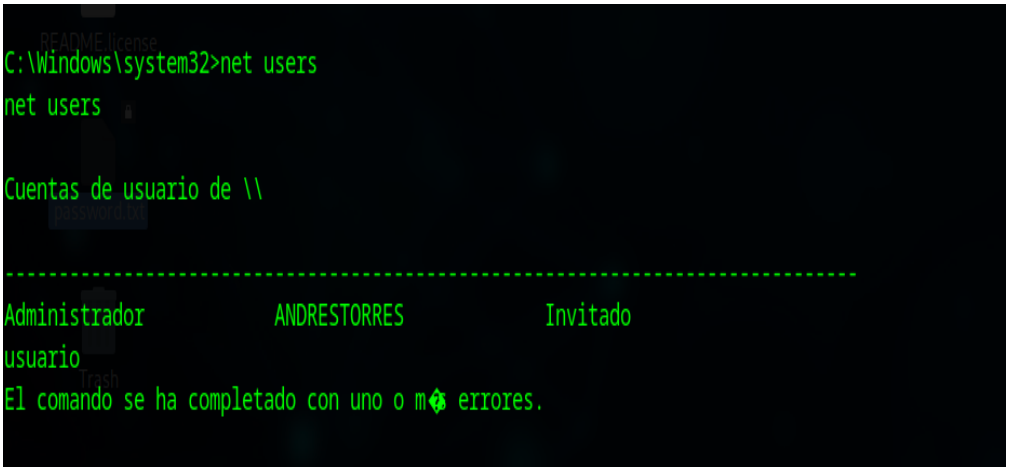
Ejecución de comando shell



Fuente, Elaboración Propia

Figura 24

Ejecución de comando net



Fuente, Elaboración Propia

Podemos confirmar en la máquina de Windows 7 donde se ejecutaron correctamente los comandos para la creación del usuario con sus respectivos permisos de administrador

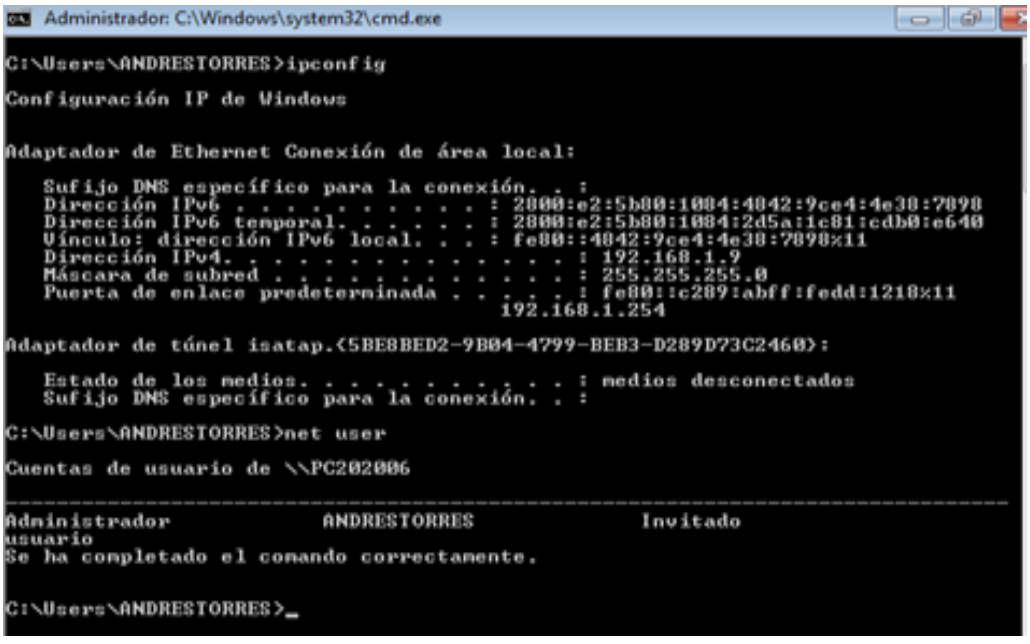
Figura 25

Maquina local Windows 7

Fuente, Elaboración Propia

Figura 26

Símbolo del sistema Windows 7



Fuente, Elaboración Propia

Identificación Del Fallo De Seguridad En La Máquina Windows

En el análisis realizado por el Red Team para identificar la causa de la fuga de información en la máquina comprometida, los siguientes datos y detalles fueron esenciales para identificar el fallo de seguridad específico que afecta al sistema Windows:

Detalles sobre la máquina comprometida

***S*istema operativo.** Se sabe que el equipo afectado ejecuta Windows, lo cual es clave para dirigir el análisis hacia las vulnerabilidades conocidas en este sistema operativo.

Aplicación vulnerable. Se menciona que una aplicación vulnerable está instalada en la máquina, aunque no se especifica el nombre. Esta información es crucial, ya que permite investigar posibles vulnerabilidades de aplicaciones en sistemas Windows y buscar exploits conocidos asociados con esta aplicación.

Exploit Asociado

Se indica que la aplicación vulnerable tiene un exploit conocido, lo que sugiere que la vulnerabilidad puede ser explotada. Esto permite investigar si la máquina es susceptible a este exploit, buscando en bases de datos de vulnerabilidades como el CVE.

Acceso Mediante Shell

Se menciona que el exploit podría llevar a un acceso remoto a través de Shell, lo que implica que el atacante podría ejecutar comandos en el sistema con privilegios limitados. Esto apunta a que la vulnerabilidad podría ser una vulnerabilidad de ejecución remota de código (RCE) o relacionada con algún servicio expuesto como SMB, RDP o SSH.

Escalamiento De Privilegios

Se está investigando también la posibilidad de escalar privilegios creando un usuario administrador. Esto indica que el atacante podría primero obtener acceso con privilegios bajos y luego aprovechar alguna vulnerabilidad o configuración débil en el sistema para ganar privilegios elevados y tomar control total del sistema.

C**opia Forense Del Servidor**

El equipo forense realizó una copia del servidor afectado, lo que permitió realizar un análisis detallado sin afectar el entorno de producción. Esto proporcionó un escenario controlado para investigar la vulnerabilidad y realizar las pruebas necesarias.

Explotación Y Poc

Se requiere que, al confirmar el fallo de seguridad, se cree un usuario administrador como parte de una Prueba de Concepto (PoC) para demostrar la efectividad del exploit. Esto implica realizar un ataque de escalada de privilegios creando un usuario con permisos de administrador para mostrar que la máquina es vulnerable**.**

Análisis Del Fallo De Seguridad

El fallo de seguridad parece estar relacionado con una vulnerabilidad explotable remotamente en la aplicación instalada en la máquina, lo que permite que un atacante obtenga acceso inicial y luego escalé sus privilegios, posiblemente mediante la creación de un usuario administrador. La combinación de una aplicación vulnerable, un exploit conocido y la posibilidad de escalada de privilegios, revela una brecha de seguridad grave que permitiría al atacante tomar el control completo del sistema.

Herramienta Utilizada Para La Identificación De Fallos De Seguridad Y Puertos Abiertos En La Máquina Windows

Para detectar las vulnerabilidades presentes en la máquina que utiliza el sistema operativo Windows, se recurrió al uso de la herramienta Nmap, especialmente con el parámetro --script vuln, que permite ejecutar scripts diseñados para identificar fallos de seguridad en servicios activos. Esta herramienta facilitó el reconocimiento de los puertos abiertos y de los servicios que podrían estar expuestos a ataques. Además, se empleó el Framework Metasploit para llevar a cabo pruebas de explotación que confirmaran la posibilidad de acceder al sistema y escalar privilegios a partir de dichas debilidades.

En relación con el puerto que utiliza la aplicación mencionada en el anexo, se determinó que esta opera a través del puerto TCP 445, correspondiente al protocolo SMB. Este puerto ha estado históricamente vinculado con vulnerabilidades críticas, como la CVE-2017-0143, que puede ser utilizada para ejecutar código malicioso de forma remota. La detección de este puerto activo fue fundamental para identificar la brecha de seguridad y avanzar en el análisis.

Descripción Del Impacto Del Ataque En La Máquina Windows

El ataque realizado contra la máquina Windows afecta su seguridad de forma crítica, comprometiendo tanto su integridad como su confidencialidad. En términos simples, el atacante aprovecha una vulnerabilidad del sistema operativo o de una aplicación específica para acceder sin autorización. Este tipo de ataque, generalmente, se inicia mediante la explotación de un puerto abierto vulnerable, como el puerto 445 (SMB), a través del cual se puede ejecutar código malicioso en el sistema remoto.

Una vez que el atacante logra explotar esta debilidad, puede tomar el control del sistema por medio de una sesión de consola o shell remota (por ejemplo, usando Meterpreter en Metasploit). Desde allí, puede realizar acciones como escalar privilegios, crear cuentas de usuario administrador, extraer información confidencial, o incluso mantener el acceso de manera persistente, lo cual pone en riesgo toda la infraestructura de la organización.

El flujo de un ataque a una máquina con Windows por parte de un equipo Red Team. El ataque comienza con el escaneo de puertos utilizando Nmap, lo que permite detectar que el puerto 445/TCP (usado por el protocolo SMB) está abierto en la máquina objetivo. El atacante luego explota la vulnerabilidad CVE-2017-0143 (EternalBlue) usando Metasploit Framework, lo que le da acceso remoto a través de Meterpreter.

A partir de ahí, el atacante puede crear un usuario administrador, escalar privilegios, y exfiltrar datos. Finalmente, establece persistencia, asegurando su acceso continuo al sistema comprometido. Este proceso resalta la importancia de parchear vulnerabilidades y monitorear activamente los sistemas para evitar compromisos similares.

Figura 27

Gráfico explicativo de ataque

Fuente, Elaboración Propia

- **Atacante.** Identifica al Red Team o atacante externo.
- **Objetivo.** Máquina Windows vulnerable detectada por escaneo.
- **Vulnerabilidad.** Exploits conocidos como EternalBlue.
- **Acceso.** Gana control del sistema y crea usuarios.
- **Impacto.** Asegura acceso.

Documentación De Los Pasos Y Metodología

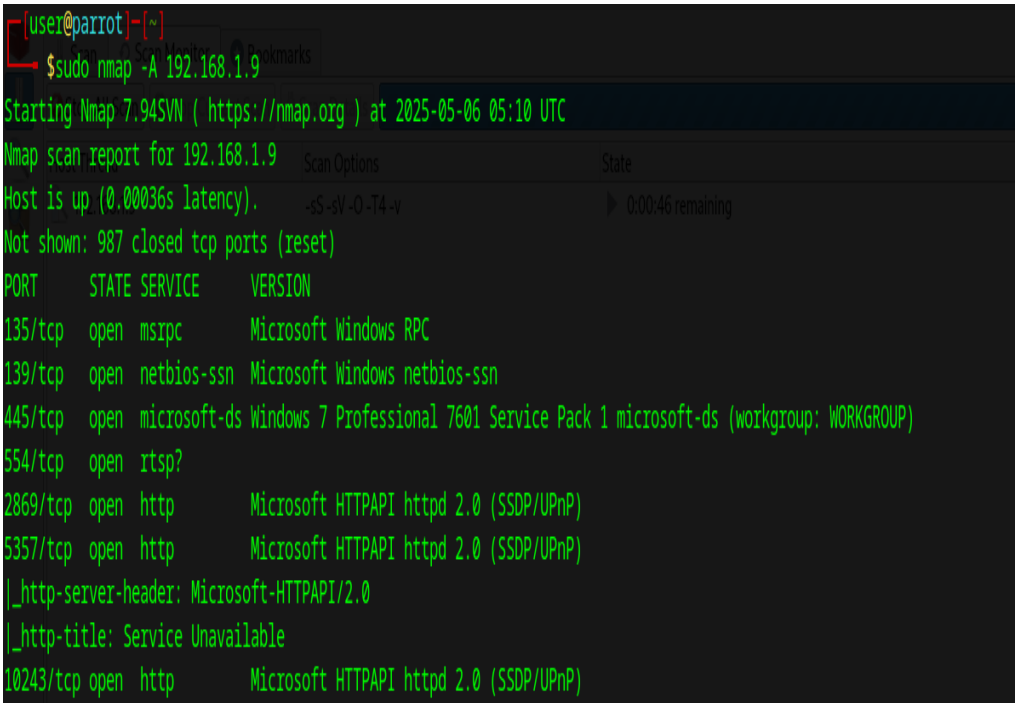
1. Escaneo De La Máquina Objetivo Con Nmap

Acción. Se inició un escaneo de puertos de la máquina objetivo utilizando el comando Nmap para identificar los puertos abiertos y los servicios activos en el sistema.

Comando ejecutado. Nmap -A 192.168.1.9

Figura 28

Comando NMAP puerto 445



Fuente, Elaboración Propia

Evidencia. En los resultados, se identificó que el puerto 445 estaba abierto, lo que indica que el protocolo SMB está activo. Este puerto es conocido por ser vulnerable a la explotación de EternalBlue, que afecta a versiones antiguas de Windows 7.

Resultado. El puerto 445 está abierto, y la máquina tiene un servicio SMB expuesto.

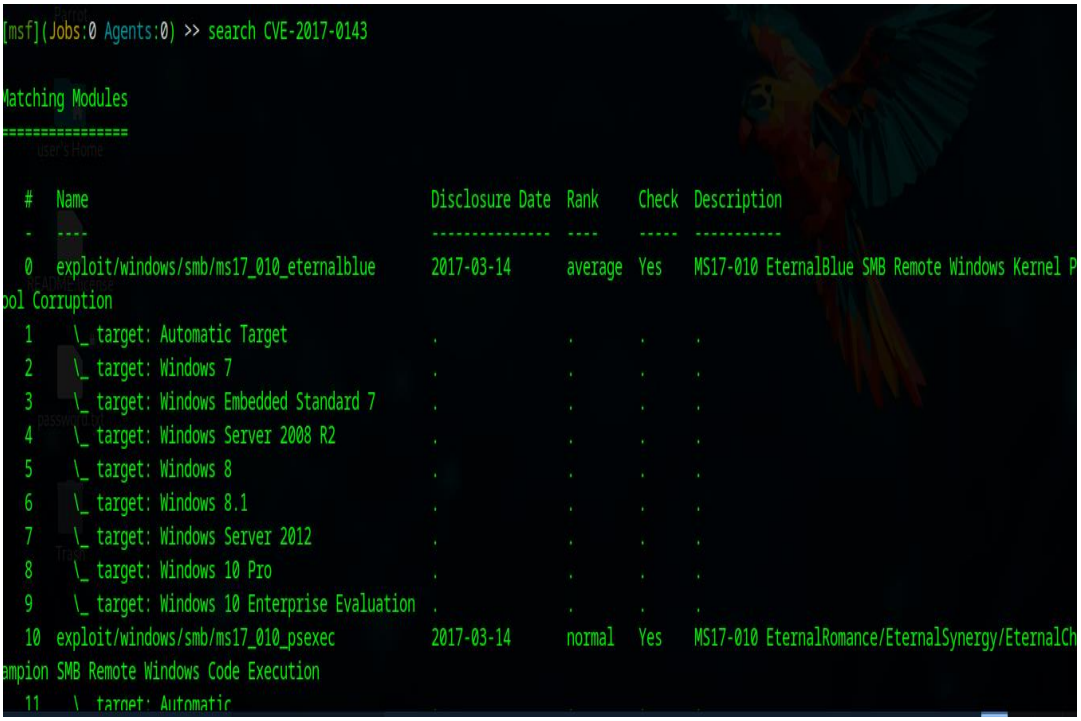
2. Detección De La Vulnerabilidad CVE-2017-0143 (Eternalblue)

Acción. Se verificó que la máquina vulnerable está utilizando una versión de SMB susceptible a la vulnerabilidad CVE-2017-0143, también conocida como EternalBlue.

Comando ejecutado en Metasploit. Msfconsole y Search CVE-2017-0143

Figura 29

Comando Search



Fuente, Elaboración Propia

Evidencia. El módulo de Metasploit específico para la explotación de EternalBlue detectó que la máquina era vulnerable y ejecutó la carga (payload) en el puerto 445.

Resultado. La vulnerabilidad CVE-2017-0143 fue explotada exitosamente, lo que permitió la ejecución remota de código en la máquina objetivo.

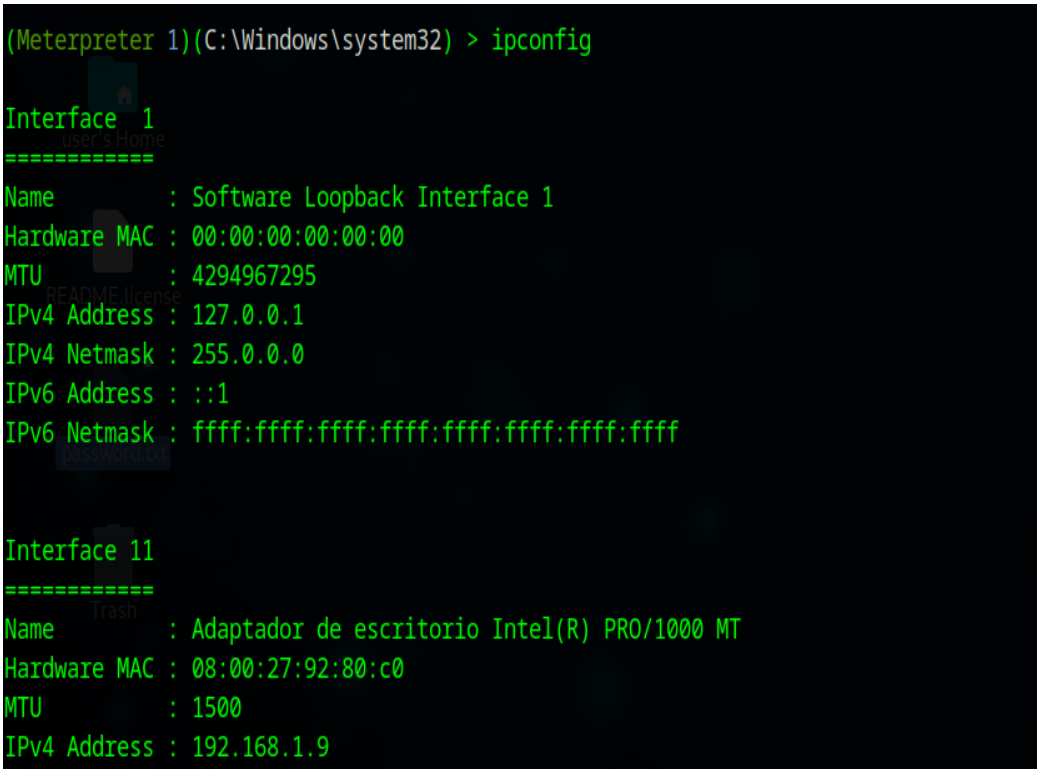
3. Acceso Remoto Usando Meterpreter

Acción. Después de explotar la vulnerabilidad, se obtuvo una shell remota usando el payload Meterpreter, lo que dio acceso al sistema comprometido.

Comando ejecutado en Metasploit. Ipconfig

Figura 30

Datos de equipo



Fuente, Elaboración Propia

Evidencia. El comando ipconfig mostró la información de la red del sistema, confirmando que se había logrado acceso exitoso a la máquina Windows 7.

Resultado. Se obtuvo información clave sobre el sistema operativo, confirmando que se trataba de un Windows 7 con la información de red.

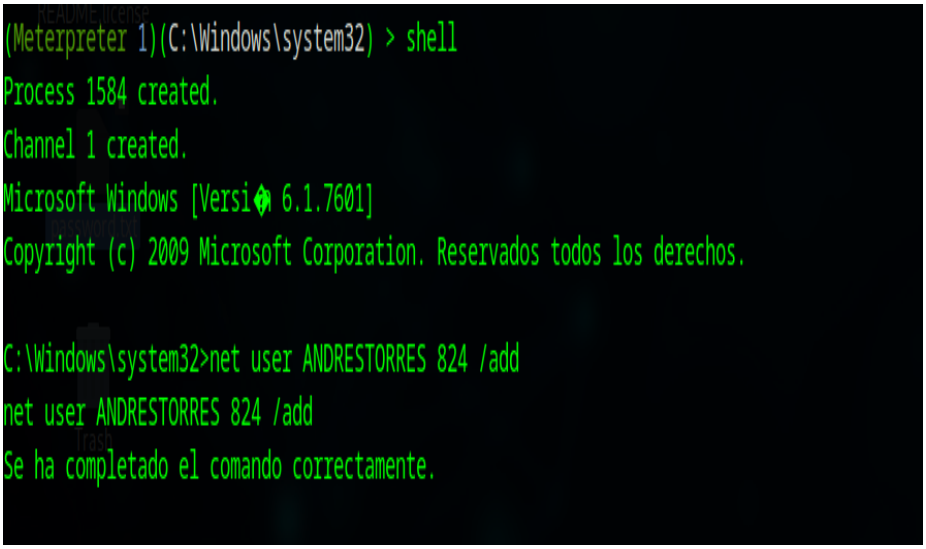
4. Escalación De Privilegios Creación De Usuario Administrador

Acción. Se escaló privilegios en el sistema creando un usuario administrador con el primer nombre y apellido para demostrar la explotación de la vulnerabilidad y la capacidad de obtener privilegios elevados.

Comando ejecutado en Meterpreter. Los comandos net user ANDRESTORRES 824 /add y net localgroup Administradores ANDRESTORRES /add son utilizados en sistemas Windows para gestionar usuarios y grupos.

Figura 31

Creación de usuario



Fuente, Elaboración Propia

Evidencia. La creación del usuario "ANDRESTORRES" con privilegios de administrador fue exitosa, como se observa en la salida del comando.

Resultado. Se creó un usuario con privilegios de administrador, demostrando la capacidad de escalar privilegios en la máquina comprometida.

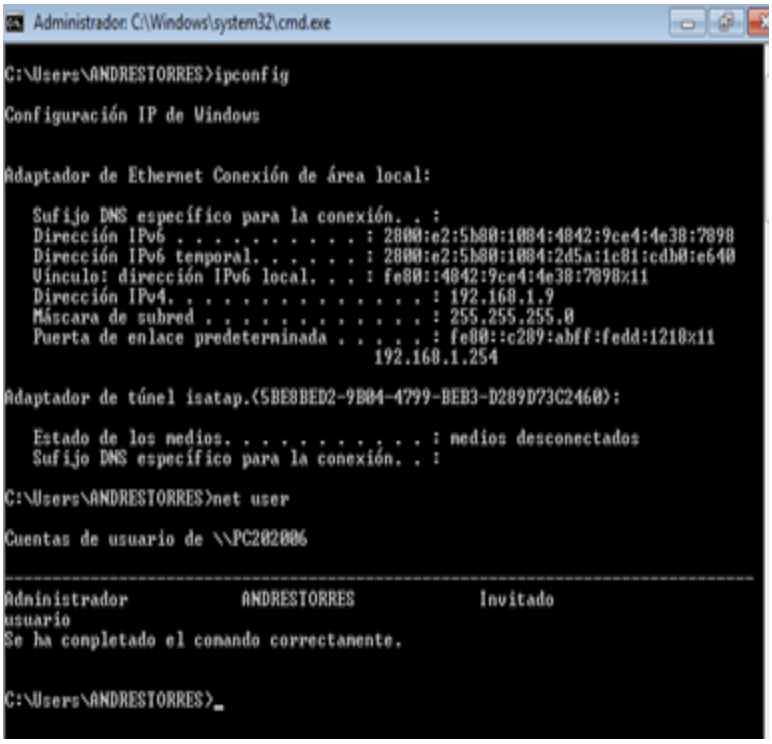
5. Impacto De Acceso

Acción. Se confirmo que se podría mantener el acceso a largo plazo con el usuario de administrador el cual nos permitirá instalar una persistencia en cada de ser necesario.

Comando ejecutado. ipconfig y net users

Figura 32

Acceso a máquina local



Fuente, Elaboración Propia

Evidencia. El comando ipconfig en sistemas Windows se utiliza para obtener detalles sobre la configuración de red de la máquina y el comando net user, por otro lado, es útil para ver las cuentas de usuario existentes en el sistema y los privilegios asociados a ellas.

Resultado. Se confirma acceso a la maquina con los comandos utilizados permitiéndonos gestionar cualquier proceso complementario en caso de ser requerido.

La metodología Red Team se empleó para simular un ataque real a una máquina Windows con el objetivo de identificar vulnerabilidades, explotar fallos de seguridad y evaluar la capacidad de la organización para detectar y defenderse de un ataque real. El proceso comenzó con el reconocimiento y escaneo de la máquina objetivo utilizando Nmap para identificar puertos abiertos y servicios activos, lo que reveló que el puerto 445 estaba expuesto, relacionado con el protocolo SMB, el cual es vulnerable a la explotación de EternalBlue. A continuación, se utilizó Metasploit para verificar la vulnerabilidad CVE-2017-0143 (EternalBlue), que afecta a versiones antiguas de Windows, y se explotó con éxito la vulnerabilidad, permitiendo la ejecución remota de código en la máquina comprometida.

Una vez que se obtuvo acceso a la máquina utilizando el payload Meterpreter, se ejecutaron comandos como ipconfig para confirmar el acceso remoto y obtener detalles sobre el sistema y la red. Posteriormente, se procedió a la escalación de privilegios creando un usuario administrador con privilegios elevados, lo que permitió al atacante tomar el control completo del sistema. Este paso demostró que el atacante no solo podía comprometer el sistema, sino también obtener control total sobre él. Finalmente, se verificó que el acceso podría mantenerse a largo plazo mediante la creación del usuario administrador, lo que proporcionó la capacidad de instalar futuros payloads o realizar otros ataques si fuera necesario.

Este enfoque de Red Team permitió simular un ataque real, identificar las vulnerabilidades críticas en el sistema y evaluar la respuesta de la organización ante un ciberataque, proporcionando información clave para mejorar las defensas y la resiliencia de la infraestructura de TI.

Etapa 4 Contención de ataques informáticos

Primeros Pasos Técnicos Frente A Un Ataque Informático En Tiempo Real

Ante la detección de un ataque cibernético en curso, es fundamental implementar una respuesta inmediata, ordenada y técnica, con el fin de contener el incidente, preservar la evidencia y restablecer la seguridad de los sistemas comprometidos. Como señalan Holdsworth y Kosinski (2024), una respuesta efectiva permite mitigar el impacto del ataque, reducir el tiempo de recuperación y evitar que el incidente se propague a otras áreas de la infraestructura.

1. Contención Inmediata Del Ataque

Objetivo. Impedir la expansión del ataque y evitar la extracción de información confidencial.

Desconectar la máquina afectada de la red, ya sea de forma física o mediante comandos como ipconfig /release, es una de las primeras acciones recomendadas para cortar la comunicación con el atacante.

Identificar procesos sospechosos en ejecución utilizando herramientas como: Process Hacker (licencia GPL), que permite visualizar procesos ocultos, DLLs inyectadas y conexiones activas y Comandos de línea como tasklist y taskkill, útiles para monitorear y finalizar procesos maliciosos.

Estas acciones están alineadas con las recomendaciones de IBM (Holdsworth & Kosinski, 2024), que destacan la contención temprana como paso clave para evitar la escalada del ataque.

2. Análisis Del Sistema Operativo

Objetivo. Detectar posibles elementos de persistencia, malware y modificaciones no autorizadas.

Analizar los programas que se ejecutan al inicio del sistema con herramientas como Autoruns.

Realizar un inventario completo del sistema mediante WinAudit (GPL).

Utilizar comandos como net user, whoami, systeminfo, wmic process list full y schtasks para recopilar información detallada del entorno.

Según el Instituto Nacional de Ciberseguridad (INCIBE, 2019), es esencial identificar elementos que hayan sido modificados por el atacante, tales como cuentas de usuario, procesos persistentes o tareas programadas, para cortar cualquier punto de reinfección.

3. Análisis De Red

Objetivo. Detectar conexiones activas, tráfico sospechoso o canales de comunicación con servidores de control (C2).

Utilizar Wireshark (GPL) para capturar y analizar paquetes de red en tiempo real.

Ejecutar el comando netstat -ano | findstr ESTABLISHED para identificar conexiones establecidas, relacionándolas con sus respectivos procesos mediante el PID.

Emplear TCPView como herramienta gráfica para observar conexiones activas de manera más visual.

Holdsworth y Kosinski (2024) explican que uno de los objetivos centrales del análisis de red es identificar cualquier canal activo de comunicación con el atacante, lo cual es vital para cortar el control remoto del sistema.

4. Recolección De Evidencia

Objetivo. Conservar información relevante para un análisis forense y posible investigación legal.

Utilizar FTK Imager Lite (gratuito) para generar imágenes forenses del disco y evitar la alteración de evidencia.

Analizar los registros del sistema con herramientas como Log Parser.

En entornos donde esté implementado, aprovechar el uso de Sysmon en conjunto con una pila de análisis como ELK Stack para correlacionar eventos.

De acuerdo con INCIBE (2019), recopilar evidencias desde el inicio del incidente permite reconstruir lo sucedido, identificar el origen y mejorar las medidas de prevención futuras.

5. Mitigación Y Recuperación

Objetivo. Eliminar accesos no autorizados y restaurar la seguridad del sistema.

Cambiar todas las contraseñas administrativas.

Deshabilitar o eliminar cuentas sospechosas.

Configurar reglas en el firewall para bloquear el tráfico malicioso.

Revisar y limpiar tareas programadas o entradas de registro alteradas.

Estas acciones forman parte de la fase de recuperación descrita por IBM (Holdsworth & Kosinski, 2024), cuyo objetivo es garantizar que el sistema regrese a un estado confiable y esté protegido frente a ataques similares en el futuro.

La respuesta ante un ataque en tiempo real debe ejecutarse de forma ágil, técnica y estructurada, priorizando la contención, el análisis detallado del entorno y la recolección adecuada de evidencia.

Medidas De Hardenización Para Prevenir Repetición De Ataques

Teniendo en cuenta el ataque realizado durante el ejercicio del Red Team, es fundamental implementar medidas específicas de hardening para mitigar vulnerabilidades y fortalecer la seguridad del sistema afectado. Estas acciones deben basarse en los estándares del Center for Internet Security (CIS) y complementarse con otras buenas prácticas reconocidas en el campo de la ciberseguridad. Según Ben Gorman (2023), es especialmente importante deshabilitar protocolos obsoletos como SMBv1, que han sido explotados por vulnerabilidades críticas como EternalBlue (CVE-2017-0143), para evitar accesos remotos no autorizados.

A continuación, se detallan algunas recomendaciones clave:

Deshabilitar SMBv1. Dado que este protocolo está obsoleto y presenta vulnerabilidades críticas —como quedó evidenciado en la explotación de EternalBlue (CVE-2017-0143)—, es imprescindible desactivarlo completamente desde la configuración del sistema o mediante políticas de grupo, evitando así que pueda ser utilizado como vector de ataque (Gorman, 2023).

Mantener el sistema actualizado. Es fundamental aplicar de forma regular los parches de seguridad y actualizaciones del sistema operativo, ya que estos corrigen vulnerabilidades conocidas que podrían ser explotadas por atacantes (Gorman, 2023).

Aplicar los lineamientos del CIS Benchmark para Windows. Este conjunto de buenas prácticas ofrece un marco para configurar adecuadamente el sistema operativo, incluyendo la desactivación de servicios innecesarios, la configuración correcta de permisos y políticas de cuenta, el endurecimiento del firewall y la restricción del uso de cuentas con privilegios elevados.

Implementar segmentación de red y control de acceso. Dividir la red en zonas de seguridad diferenciadas y establecer listas de control de acceso limita la movilidad lateral del atacante dentro de la infraestructura, dificultando la propagación del ataque.

Habilitar y configurar adecuadamente el firewall. Es esencial que el firewall esté activo y que sus reglas bloqueen puertos comúnmente explotados, como los puertos 445, 139 y 135, utilizados por protocolos vulnerables como SMB.

Establecer políticas de contraseñas seguras. Definir requisitos estrictos en cuanto a complejidad, longitud mínima, expiración periódica y bloqueo tras múltiples intentos fallidos ayuda a prevenir accesos no autorizados mediante técnicas de fuerza bruta o robo de credenciales.

Activar la auditoría de eventos del sistema. Registrar y monitorear eventos de seguridad permite detectar comportamientos anómalos o intentos de intrusión en tiempo real, especialmente cuando se utilizan soluciones de monitoreo centralizado como SIEM (Security Information and Event Management).

Eliminar o desactivar cuentas innecesarias o por defecto. Las cuentas que no se usan o las que vienen por defecto pueden representar un riesgo si son comprometidas, por lo que deben ser gestionadas, eliminadas o deshabilitadas según corresponda.

Aplicar el principio de privilegios mínimos. Los usuarios deben disponer únicamente de los permisos estrictamente necesarios para cumplir sus funciones, limitando así el alcance de cualquier posible compromiso.

Utilizar soluciones de seguridad avanzadas (EDR/antivirus). Herramientas de detección y respuesta en endpoints (EDR) y antivirus modernos permiten identificar, bloquear y responder rápidamente a amenazas sofisticadas, manteniendo la integridad y disponibilidad del sistema.

Estas medidas combinadas permiten reducir de manera significativa la superficie de ataque, dificultar el acceso no autorizado y fortalecer la postura general de ciberseguridad de la organización, protegiendo así los activos críticos frente a amenazas similares a las simuladas durante el ejercicio de Red Team (Gorman, 2023).

Análisis De Las Diferencias Entre Blue Team Y Equipo De Respuesta A Incidentes

El Blue Team es el equipo técnico especializado en la defensa diaria y continua de la infraestructura informática. Aunque originalmente el Blue Team se enfocaba en la respuesta a incidentes, en la actualidad su rol se amplía para incluir tareas preventivas como el monitoreo constante, fortalecimiento de controles de seguridad, análisis de vulnerabilidades, aplicación de parches y simulacros de defensa. (Sánchez, 2021).

.Por otro lado, el equipo de respuesta a incidentes informáticos (CSIRT, por sus siglas en inglés), es una estructura diseñada para actuar de forma reactiva frente a incidentes de seguridad. Originalmente, este tipo de equipos eran conocidos como CERT, pero debido a derechos registrados por una entidad estadounidense, en Europa adoptamos el término CSIRT, que cumple la misma función. La misión principal de un CSIRT es recibir, analizar y coordinar respuestas a incidentes informáticos reportados por comunidades, empresas u otras entidades. Esto incluye analizar malware, investigar cómo ocurrió un ataque, ayudar a restaurar sistemas afectados y gestionar vulnerabilidades detectadas (Sánchez, 2021).

Mientras que el CSIRT coordina y gestiona la respuesta global a incidentes de seguridad, el Blue Team trabaja de manera constante para proteger, detectar y prevenir esos incidentes a nivel operativo y técnico. Ambos equipos son complementarios y esenciales para una estrategia de ciberseguridad robusta.

Uso del CIS (Center for Internet Security) dentro de un Equipo Blue Team

En un equipo Blue Team me indican que debo trabajar con el CIS (Center for Internet Security), utilizaría esta herramienta para fortalecer la ciberseguridad de los sistemas y redes de la organización mediante la adopción de buenas prácticas, controles y estándares reconocidos a nivel internacional.El CIS es una organización sin fines de lucro cuyo objetivo es reducir los ciberriesgos. Para ello, ha desarrollado dos herramientas principales: los controles CIS y los benchmarks CIS.

Estos recursos proporcionan a los responsables de sistemas y analistas de seguridad un conjunto de metodologías y recomendaciones basadas en la experiencia global de expertos, facilitando la protección y la resiliencia frente a las amenazas digitales.

De acuerdo con el equipo de Ciber 4 All Team (2022), los controles CIS comprenden 18 acciones fundamentales que las organizaciones deben implementar para reforzar su defensa contra ataques cibernéticos se detalla a continuación:

Inventario y control de activos empresariales. Identificar y gestionar todos los activos tecnológicos para asegurar que estén protegidos.

Inventario y control de activos de software. Mantener un control riguroso de los programas instalados para prevenir software no autorizado.

Protección de datos. Implementar medidas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Configuración segura de activos y software empresariales. Hay que asegurar que los sistemas y aplicaciones tengan configuraciones seguras para minimizar vulnerabilidades.

Gestión de cuentas. Controlar y administrar las cuentas de usuario para evitar accesos no autorizados.

Gestión del control de acceso. Implementar políticas estrictas de acceso basado en el principio de menor privilegio.

Gestión continua de vulnerabilidades. Detectar y corregir vulnerabilidades en los sistemas de manera constante.

Gestión de registros de auditoría. Mantener registros detallados para facilitar la detección y análisis de incidentes.

Protección de correo electrónico y navegador web. Implementar defensas específicas para estos vectores comunes de ataque.

Defensas contra malware. Desplegar soluciones efectivas para prevenir, detectar y eliminar software malicioso.

Recuperación de datos. Establecer mecanismos para restaurar información y sistemas tras un incidente.

Gestión de infraestructura de red. Proteger y controlar los dispositivos y servicios de red para evitar intrusiones.

Monitoreo y defensa de redes. Implementar sistemas de monitoreo continuo para detectar actividades sospechosas.

Formación en habilidades y concienciación sobre seguridad. Capacitar al personal para que reconozca y evite riesgos de seguridad.

Gestión de proveedores de servicios. Evaluar y controlar la seguridad de terceros que acceden a los sistemas.

Seguridad del software de aplicación. Aplicar buenas prácticas para el desarrollo seguro y la evaluación de aplicaciones.

Gestión de respuesta a incidentes. Definir procedimientos claros para responder rápida y eficazmente ante incidentes.

Pruebas de penetración. Realizar simulaciones controladas para identificar y corregir vulnerabilidades antes que los atacantes reales.

Entre las acciones se incluyen el inventario y control de activos, la gestión continua de vulnerabilidades, la defensa contra malware, las pruebas de intrusión y la protección de datos. (Center for Internet Security, 2025).

Por otro lado, los benchmarks CIS son guías específicas para la configuración segura de software, hardware y sistemas operativos (como Windows, Linux, servidores, proveedores cloud y dispositivos móviles), que ofrecen directrices detalladas para aplicar las mejores prácticas de seguridad conforme a los controles CIS. Estas guías facilitan la configuración correcta y minimizan las vulnerabilidades en infraestructuras críticas. (Center for Internet Security, 2025).

Además, la automatización juega un papel fundamental, ya que permite auditorías continuas, una gestión eficiente de los cambios y asegura el cumplimiento constante de las medidas de seguridad, mejorando la productividad y disminuyendo la posibilidad de errores humanos.

En consecuencia, el CIS se convierte en una herramienta esencial para que un equipo Blue Team proteja eficazmente los activos tecnológicos de la organización, alineándose con las mejores prácticas y estándares internacionales de ciberseguridad (Ciber 4 All Team, 2022).

Funciones Y Características Esenciales De Un Sistema SIEM

La dependencia creciente de la tecnología y del uso intensivo de Internet para actividades empresariales correo electrónico, aplicaciones y almacenamiento en la nube expone a las organizaciones a un amplio abanico de amenazas. Para contrarrestar este escenario, los sistemas SIEM (Security Information and Event Management) se han convertido en el pilar de la ciberdefensa corporativa. A continuación, se presentan sus funciones y características principales.

¿Qué Es Un SIEM?

Según Ambit Iberia Team (29 de abril de 2021), un SIEM es una plataforma de seguridad que integra dos disciplinas tradicionales:

SIM (Security Information Management). centraliza y almacena en tiempo real los registros de seguridad, facilitando su interpretación y auditoría.

SEM (Security Event Management). analiza eventos de seguridad sobre la marcha, detectando patrones anómalos y emitiendo alertas inmediatas.

La combinación de ambas capacidades proporciona una visión completa de todos los eventos de TI, lo que permite detectar, investigar y responder con rapidez y precisión ante incidentes, ofreciendo visibilidad, agilidad y capacidad de reacción ante las amenazas más sofisticadas. Su correcta implementación no solo mejora la detección y mitigación de incidentes, sino que también asegura el cumplimiento normativo y optimiza los recursos humanos y tecnológicos de la organización (Ambit Iberia Team, 2021).

Funciones Principales

Captura y normalización de datos. Recoge registros de diversas fuentes firewalls, routers, IDS/IPS, servidores, aplicaciones, endpoints, etc. y los unifica en un formato estándar para su análisis.

Almacenamiento y gestión centralizada. Conserva grandes volúmenes de logs en una base de datos escalable, aplicando políticas de retención acordes a requisitos legales y forenses.

Correlación y análisis de eventos. Relaciona sucesos aparentemente aislados mediante reglas y patrones predefinidos o personalizados, identificando secuencias de ataque complejas.

Generación de alertas y notificaciones. Supervisa continuamente la actividad de la red y de los sistemas, enviando avisos en tiempo real cuando se detectan indicadores de compromiso o infracciones de políticas.

Respuesta automatizada (SOAR). Ejecuta flujos de trabajo automáticos bloqueo de IP, cuarentena de endpoints, desactivación de cuentas comprometidas reduciendo drásticamente los tiempos de reacción.

Investigación forense y triage. Reconstruye la línea temporal de un incidente quién, cómo, cuándo y dónde y evalúa el alcance de la brecha para planificar la contención.

Informes y cumplimiento normativo

Genera reportes estándar o personalizados para normativas como ISO 27001, PCI-DSS, GDPR y HIPAA, documentando auditorías y conservando registros históricos.

Características Distintivas

Visibilidad unificada. Consolida todos los eventos de seguridad en un único panel de control, ofreciendo una visión global de la postura defensiva.

Escalabilidad y alta disponibilidad. Procesa desde megabytes hasta terabytes de datos diarios, con tolerancia a fallos mediante clustering y balanceo de carga.

Motor de reglas flexible. Incluye bibliotecas de casos de uso preconfigurados y permite crear reglas propias adaptadas a los riesgos particulares de la organización.

Búsqueda ad hoc y análisis avanzado. Facilita consultas en lenguaje libre sobre el histórico de eventos para investigaciones puntuales y descubrimiento de nuevos patrones.

Integración con inteligencia de amenazas. Consume feeds de reputación de IPs, dominios y hashes de malware, enriqueciendo los eventos y anticipando amenazas emergentes.

Automatización de tareas repetitivas. Libera al equipo de seguridad de labores manuales escaneos, monitorización continua para que se concentren en actividades de mayor valor estratégico.

Documentación trazable. Registra cada fase del ciclo de vida de un incidente detección, contención, erradicación y recuperación generando una base de conocimiento que optimiza respuestas futuras.

Tres Herramientas Clave De Contención Para Ataques Informáticos

A continuación, se describen tres herramientas de contención que, más allá de la detección, bloquean o aíslan activamente los ataques en tiempo real (Teijeiro, 2024):

1. Pfsense (Firewall De Red)

pfSense es un software de código abierto que puede instalarse en hardware dedicado o como appliance virtual. Opera "inline" en el perímetro de la red, filtrando el tráfico de entrada y salida mediante reglas basadas en puertos, protocolos y direcciones IP. Cuando detecta paquetes maliciosos o no autorizados, los descarta antes de que alcancen su destino. Además, permite la integración con módulos adicionales como pfBlockerNG, Snort o Suricata para ampliar sus capacidades de contención (Teijeiro, 2024).

2. Suricata (Sistema De Prevención De Intrusiones – IPS)

Suricata es un motor de inspección profunda de paquetes (DPI) de código abierto, compatible con las reglas de Snort, que puede desplegarse en hardware dedicado o integrarse en routers y firewalls. Funcionando en línea con el flujo de red, analiza cada paquete en busca de firmas de exploits o comportamientos maliciosos y bloquea automáticamente aquellos que representen una amenaza, como intentos de inyección de código o escaneos de puertos. Destaca por su arquitectura multihilo de alto rendimiento y su capacidad de captura de paquetes para análisis forense posterior (Teijeiro, 2024).

3. Symantec Endpoint Protection (Antivirus Con Capacidades De Contención)

Symantec Endpoint Protection es un agente de software instalado en estaciones de trabajo y servidores. Además de emplear firmas y heurística para detectar malware, cuarentena automáticamente los archivos o procesos sospechosos, bloquea su ejecución y puede aislar el endpoint afectado de la red corporativa hasta que se confirme su limpieza.

Ofrece protección en tiempo real respaldada por inteligencia artificial y puede revocar conexiones de red o deshabilitar servicios comprometidos para evitar la propagación de la amenaza (Teijeiro, 2024).

Cada una de estas soluciones actúa de manera proactiva e inmediata sobre el flujo de datos o el comportamiento del sistema para contener las amenazas en el momento en que se detectan. Esto significa que no solo identifican el riesgo, sino que también implementan mecanismos para bloquear, aislar o mitigar el ataque, evitando que se propague a otros sistemas o recursos críticos dentro de la infraestructura tecnológica. Al limitar esta propagación, se reduce el impacto potencial y se protege la integridad y disponibilidad de los activos. Además, estas herramientas brindan al equipo de seguridad el tiempo necesario para realizar un análisis exhaustivo del incidente, comprender su alcance y origen, y diseñar una estrategia de remediación adecuada. De esta forma, se mejora la capacidad de respuesta y se minimizan los daños tanto técnicos como operativos, fortaleciendo la postura general de ciberseguridad de la organización.

Etapa 5 Socialización De Informe Técnico

Aspectos En La Construcción De Estrategias Ofensivas Y Defensivas En Ciberseguridad

Para desarrollar estrategias efectivas en los equipos Red Team y Blue Team, es esencial comprender a fondo tanto las técnicas ofensivas como las defensivas. El Red Team se enfoca en tareas como el reconocimiento del entorno, la simulación de amenazas avanzadas, el uso de marcos como MITRE ATT&CK, la evasión de controles defensivos y la elaboración de informes detallados. Por su parte, el Blue Team se encarga de la vigilancia continua mediante herramientas como SIEM, la respuesta ágil a incidentes, el análisis forense, la aplicación de parches y la capacitación constante del personal. Estas prácticas, cuando se integran de manera colaborativa, permiten una defensa más robusta frente a ciber amenazas (Dale, 2025).

Red Team

1. Reconocimiento y análisis del entorno. Identificación de activos, servicios y posibles vectores de ataque.

2. Simulación de amenazas reales y sofisticadas. Reproducción de tácticas utilizadas por atacantes avanzados (APT).

3. Uso de tácticas, técnicas y procedimientos (TTPs). Basados en marcos como MITRE ATT&CK.

4. Evasión de controles de seguridad. Desarrollo de técnicas para evitar la detección por parte del Blue Team.

5. Elaboración de informes detallados. Análisis de hallazgos y recomendaciones específicas para mejorar la seguridad.

Blue Team

1.Monitoreo constante de la infraestructura. Implementación de soluciones SIEM y otras herramientas de detección.

2. Gestión de incidentes eficiente. Respuesta rápida ante intrusiones y recuperación segura.

3. Análisis forense digital. Investigación detallada de eventos de seguridad para determinar el origen y alcance de los ataques.

4. Aplicación de parches y refuerzo de sistemas. Mantenimiento proactivo para reducir superficies de ataque.

5. Capacitación continua. Simulacros y ejercicios que mejoran la preparación ante amenazas reales.

La implementación coordinada de estrategias entre los equipos Red Team y Blue Team es esencial para construir una defensa cibernética sólida y resiliente. Mientras el Red Team identifica vulnerabilidades mediante simulaciones ofensivas avanzadas, el Blue Team fortalece la infraestructura mediante monitoreo, respuesta y mejora continua. Como señala Dale (2025), solo a través de una comprensión mutua y una colaboración efectiva entre ambos enfoques es posible anticipar, detectar y mitigar amenazas de manera proactiva, elevando así la postura de seguridad de toda la organización.

Enlace Al Video De Sustentación

Vinculo del video

Recomendaciones

Fortalecer la seguridad en una organización requiere un enfoque integral y proactivo que combine tecnología, procesos y formación del personal. Según AGE2 (2025), prevenir brechas de seguridad no solo protege los activos clave, sino que también preserva la reputación corporativa y garantiza la continuidad del negocio. A partir de esta idea, se sugieren las siguientes recomendaciones estratégicas:

Evaluación Completa De Riesgos

Identificar y evaluar constantemente los activos más valiosos y las amenazas potenciales permite priorizar las acciones de seguridad. AGE2 (2025) destaca que este es un paso fundamental para anticipar ataques y adaptar las medidas de defensa a las necesidades específicas de la organización.

Promover Una Cultura De Ciberseguridad

El factor humano sigue siendo uno de los eslabones más débiles en la seguridad. Por ello, AGE2 (2025) enfatiza la importancia de capacitar continuamente al personal y realizar simulaciones de ataques, como phishing, para fortalecer la conciencia y las buenas prácticas en seguridad digital.

Implementar Controles De Acceso Estrictos Y El Modelo Zero Trust

Aplicar la autenticación multifactor y políticas de acceso basado en el mínimo privilegio reduce significativamente el riesgo de accesos no autorizados. AGE2 (2025) resalta el modelo Zero Trust, que verifica todas las solicitudes de acceso, tanto internas como externas, como una estrategia clave para reforzar la seguridad.

Cifrado De Información Sensible

El cifrado asegura que los datos, incluso si son interceptados, no puedan ser leídos sin la clave correspondiente. AGE2 (2025) menciona tecnologías emergentes como el cifrado y enfoques centrados en los datos como elementos esenciales para proteger la información, especialmente en entornos de nube.

Monitoreo Constante Y Automatización En La Respuesta

Contar con herramientas que permitan detectar y responder automáticamente a amenazas es vital. AGE2 (2025) recomienda el uso de soluciones como XDR (Extended Detection and Response) para acelerar la reacción ante incidentes y minimizar daños.

Desarrollar Planes De Respuesta Ante Incidentes Y Realizar Simulacros Regulares

Contar con un plan claro para contener y mitigar ataques permite actuar de manera rápida y organizada. AGE2 (2025) sugiere incluir simulaciones de crisis cibernéticas para fortalecer la preparación y coordinación de todos los equipos involucrados.

Evaluar La Seguridad De Terceros Y La Cadena De Suministro

Las amenazas externas, como las provenientes de proveedores, representan un riesgo creciente. Por ello, AGE2 (2025) recomienda realizar evaluaciones rigurosas a terceros que tengan acceso a sistemas o datos críticos, implementando políticas estrictas de seguridad.

Estas recomendaciones, combinadas, ayudan a construir un sistema de seguridad robusto, adaptable a nuevas amenazas y capaz de proteger los activos más valiosos de la organización. La clave está en integrar tecnología avanzada con una estrategia de mejora continua y una cultura organizacional centrada en la ciberseguridad.

Conclusiones

La ciberseguridad debe abordarse como un proceso continuo de aprendizaje, en el que los profesionales deben mantenerse actualizados frente a las nuevas amenazas, herramientas y técnicas utilizadas por los atacantes. La naturaleza dinámica del entorno digital exige una actitud proactiva y adaptable, en la que el aprendizaje constante se convierte en un pilar esencial para prevenir, detectar y responder efectivamente a incidentes de seguridad.

La integración de enfoques ofensivos (Red Team) y defensivos (Blue Team) favorece una comprensión holística del ecosistema de amenazas. Al simular ataques reales y analizar la eficacia de las defensas, se genera un conocimiento práctico que permite identificar debilidades, mejorar controles y fortalecer la arquitectura de seguridad. Este enfoque dual también promueve la colaboración entre equipos, lo cual resulta clave para el desarrollo de estrategias más eficaces y adaptativas.

La transformación digital y creciente dependencia de las tecnologías de la información, la existencia de un marco normativo robusto como la Ley 1273 de 2009 en Colombia representa un paso decisivo hacia la consolidación de un entorno cibernético más seguro. Esta legislación establece con precisión las conductas ilícitas en el ámbito digital, como el acceso no autorizado, el sabotaje informático y la interceptación de datos, lo que permite una actuación judicial más efectiva frente a los delitos informáticos.

La formación y concientización del talento humano es fundamental para fortalecer la postura de seguridad de cualquier organización. Las personas siguen siendo uno de los eslabones más vulnerables en la cadena de seguridad, por lo que es crucial desarrollar programas educativos y campañas de sensibilización que les permitan identificar riesgos, adoptar buenas prácticas y actuar con responsabilidad frente al uso de los recursos tecnológicos.

La investigación y análisis de incidentes reales proporciona una base sólida para generar conocimiento aplicado, ya que permite entender el contexto, el impacto y las tácticas empleadas por los atacantes. Esta información es clave para la retroalimentación de los procesos de seguridad, el rediseño de políticas internas y el fortalecimiento de las capacidades de respuesta. Además, contribuye al desarrollo de modelos predictivos y estrategias preventivas más precisas.

El enfoque interdisciplinario en ciberseguridad, que combina aspectos técnicos, legales y organizacionales, enriquece la construcción del conocimiento al permitir una visión más completa de los riesgos y soluciones posibles. La colaboración entre expertos en tecnología, derecho, gestión y comunicación es esencial para diseñar estrategias que no solo protejan los sistemas, sino que también cumplan con las normativas, respeten los derechos de los usuarios y se alineen con los objetivos institucionales.

A lo largo de las pruebas realizadas en el entorno comprometido, la capacidad de mantener la persistencia y el control del sistema a través de técnicas como la creación de usuarios administradores o el uso de herramientas como Metasploit, demuestra la importancia de un enfoque integral en la defensa y protección de los sistemas. La implementación de medidas como la persistencia asegura que, incluso después de un reinicio o un cierre de sesión, los atacantes mantengan acceso a los sistemas comprometidos, lo que subraya la necesidad de medidas proactivas y de seguridad constante para proteger los activos digitales.

El uso de herramientas especializadas en ciberseguridad, tales como escáneres de vulnerabilidades (como Open VAS o Nessus), cortafuegos (firewalls) y sistemas de detección y prevención de intrusos (IDS/IPS), se vuelve esencial en un ecosistema digital donde los ataques pueden surgir de múltiples vectores.

Estas soluciones tecnológicas permiten implementar medidas de protección en tiempo real, automatizar procesos de monitoreo, y responder de manera eficaz a incidentes de seguridad. En conjunto, su aplicación mejora significativamente la gestión del riesgo operativo y fortalece la resiliencia de las organizaciones ante ciber amenazas.

La ciberseguridad, más allá de ser un conjunto de herramientas técnicas, representa un campo dinámico que requiere una construcción constante de conocimiento a partir de la experiencia, la formación interdisciplinaria y la colaboración entre equipos ofensivos y defensivos. Comprender las amenazas, fortalecer las capacidades humanas, analizar incidentes reales y adaptarse al cambio tecnológico son elementos esenciales para desarrollar estrategias efectivas que garanticen la protección de los activos digitales en cualquier organización.

Referencias Bibliográficas

AGE2. (2025, 26 de mayo). *Seguridad empresarial: prevenir brechas*. https://www.age2.es/noticias/seguridad-empresarial-prevenir-brechas

Ambit Iberia Team. (2021, 29 de abril). *¿Qué significa SIEM y cómo funciona?* Ambit Iberia. https://www.ambit-iberia.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

CEH v11 Certified Ethical Hacker Study Guide. (s. f.). *Wiley eBooks | IEEE Xplore*. https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/book/9946651

Center for Internet Security. (2025). *The 18 CIS critical security controls*. https://www.cisecurity.org/controls/cis-controls-list

Dale, C. (2025, 26 de mayo). *Purple, blue and red teaming*. Fortra. https://www.fortra.com/es/recursos/guias/purple-blue-red-teaming

Ciber 4 All Team. (2022, 20 de enero). *Controles CIS: las mejores prácticas en ciberseguridad*. Tarlogic. https://www.tarlogic.com/es/blog/controles-cis-ciberseguridad/

Congreso de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado "protección de la información y de los datos"*. Diario Oficial No. 47.223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CSIRT Académico UNAD. (s. f.). *Centro de Respuestas a Incidentes Informáticos CSIRT Académico UNAD*. https://csirt.unad.edu.co

Delta Asesores. (2023). *Ley de delitos informáticos en Colombia*. https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Greenbone. (s. f.). *OpenVAS*. https://www.greenbone.net

Herzog, P. (2010). *OSSTMM - Open Source Security Testing Methodology Manual* (v3). ISECOM. https://www.isecom.org/OSSTMM.3.pdf

Holdsworth, J., & Kosinski, M. (2024, 20 de agosto). *¿Qué es la respuesta a incidentes?* IBM. https://www.ibm.com/es-es/topics/incident-response

INCIBE. (2019, 7 de marzo). *Primeros pasos en la respuesta a incidentes*. Instituto Nacional de Ciberseguridad de España. https://www.incibe.es/empresas/blog/primeros-pasos-respuesta-incidentes

Gorman, B. (2023, 22 de septiembre). *¿Qué es EternalBlue?* AVG. https://www.avg.com/es/signal/eternal-blue

International Organization for Standardization. (2013). *ISO/IEC 27001:2013*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (s. f.). *Guía de seguridad digital para empresas*. https://www.mintic.gov.co/

MITRE. (s. f.). *CVE - Common Vulnerabilities and Exposures*. https://cve.mitre.org

National Institute of Standards and Technology (NIST). (2020). *NIST SP 800-115: Technical guide to information security testing and assessment*. https://www.nist.gov/privacy-framework/nist-sp-800-115

Nmap.org. (s. f.). *Nmap: The Network Mapper*. https://nmap.org

Offensive Security. (s. f.). *Exploit Database*. https://www.exploit-db.com

OWASP. (s. f.). *WSTG - v4.2 | Web Security Testing Guide*. https://owasp.org/www-project-web-security-testing-guide/v42/

PTES. (2022). *The Penetration Testing Execution Standard Documentation*. https://www.pentest-standard.org

Rapid7. (s. f.). *Metasploit Framework*. https://www.rapid7.com/products/metasploit

Sánchez, J. (2021, 29 de julio). *El CSIRT y el trabajo de un Blue Team*. CodeSpace Academy. https://codespaceacademy.com/csirt-trabajo-blueteam/

Zotero. (s. f.). *Your personal research assistant*. https://www.zotero.org/