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

Nelson Javier Castelblanco Avila

Asesor

Luis Fernando Zambrano Hernández

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2025

_____

Luis Fernando Zambrano Hernández

_____ _____

Jurado Jurado

2025

Dedicatoria

A mi amada esposa, por su incondicional apoyo y su constante aliento. A mis hijas por ser la razón de mi mayor alegría y motivación.

Agradecimientos

Quiero expresar mi agradecimiento a mi familia por su paciencia y ánimo en todo momento, a los tutores de la especialización por compartir sus conocimientos y a mis compañeros por su colaboración y apoyo mutuo.

Resumen

El presente informe técnico detalla las capacidades y metodologías esenciales para equipos de ciberseguridad ofensivos (Red Team) y defensivos (Blue Team). Se inicia con la identificación del marco legal colombiano aplicable a delitos informáticos y protección de datos. Posteriormente, se describe el ejercicio de pentesting, incluyendo sus fases y herramientas clave como Nmap, Metasploit y OpenVAS, además de servicios como ExploitDB y CVE. El documento guía la implementación de un entorno virtualizado para prácticas de pentesting, seguido de un análisis ético y legal de escenarios propuestos, evaluando posibles infracciones a la Ley 1273 y al código de ética de COPNIA. Se desarrolla un caso práctico de Red Team, explotando la vulnerabilidad CVE-2017-0143 (EternalBlue) en un sistema Windows 7, documentando cada paso. Finalmente, se abordan estrategias de Blue Team, incluyendo la respuesta a incidentes en tiempo real, medidas de hardenización, la diferenciación con equipos de respuesta a incidentes, la aplicación de marcos como CIS Benchmarks y el rol de herramientas SIEM en la detección y contención de amenazas.

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

Abstract

This technical report details the essential capabilities and methodologies for offensive (Red Team) and defensive (Blue Team) cybersecurity teams. It begins by identifying the Colombian legal framework applicable to cybercrime and data protection. Subsequently, the pentesting exercise is described, including its phases and key tools such as Nmap, Metasploit, and OpenVAS, as well as services like ExploitDB and CVE. The document guides the implementation of a virtualized environment for pentesting practices, followed by an ethical and legal analysis of proposed scenarios, evaluating possible infractions of Law 1273 and the COPNIA code of ethics. A practical Red Team case is developed, exploiting the CVE-2017-0143 (EternalBlue) vulnerability in a Windows 7 system, documenting each step. Finally, Blue Team strategies are addressed, including real-time incident response, hardening measures, differentiation from incident response teams, the application of frameworks like CIS Benchmarks, and the role of SIEM tools in threat detection and containment.

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

Tabla de contenido

Lista de Figuras

Lista de Tablas

Introducción

En la era digital contemporánea, la ciberseguridad ha trascendido su rol técnico para convertirse en un pilar fundamental de la estrategia y continuidad operativa de cualquier organización. La proliferación de amenazas cibernéticas, cada vez más sofisticadas y persistentes, exige un enfoque proactivo y especializado en la protección de los activos de información. En este contexto, los equipos estratégicos de ciberseguridad, conocidos como Red Team (ofensivo) y Blue Team (defensivo), desempeñan roles cruciales y complementarios.

El presente informe técnico se adentra en el universo de estos equipos, explorando las capacidades técnicas, el marco legal y los principios éticos que rigen su actuación. Se busca no solo definir sus funciones, sino también evidenciar, mediante la aplicación práctica, las metodologías y herramientas que emplean para simular ataques, identificar vulnerabilidades y, consecuentemente, proponer estrategias robustas para el endurecimiento de los sistemas y la defensa de las infraestructuras tecnológicas. A lo largo de este documento, se analizarán desde la legislación colombiana aplicable hasta la ejecución detallada de pruebas de penetración y la implementación de contramedidas, con el fin de construir un conocimiento integral sobre cómo estos equipos contribuyen al fortalecimiento del entorno digital organizacional.

Justificación

La creciente dependencia de las tecnologías de la información y las comunicaciones (TIC) en todos los sectores productivos y sociales ha traído consigo una exposición sin precedentes a riesgos cibernéticos. Las organizaciones, independientemente de su tamaño o naturaleza, son objetivos potenciales de actores maliciosos que buscan comprometer la confidencialidad, integridad y disponibilidad de sus activos digitales. Ante este panorama, la formación de expertos con una comprensión profunda de las tácticas ofensivas (Red Team) y las estrategias defensivas (Blue Team) es imperativa.

Este trabajo se justifica en la necesidad de consolidar y aplicar conocimientos especializados que permitan no solo reaccionar ante incidentes de seguridad, sino anticiparlos y mitigarlos eficazmente. Al explorar los fundamentos legales, éticos y técnicos de los equipos de ciberseguridad, y al desarrollar habilidades prácticas en la identificación y explotación controlada de vulnerabilidades, así como en la implementación de medidas de fortalecimiento, se contribuye directamente a la profesionalización del campo. Este informe busca, por tanto, servir como un compendio aplicado que refleje la pericia necesaria para abordar los desafíos actuales de la seguridad informática y para diseñar entornos digitales más resilientes y seguros, alineados con las mejores prácticas y las tendencias del sector.

Objetivos

Objetivo General

Construir un informe técnico que permita evidenciar técnicas de Red Team & Blue Team para el endurecimiento y fortalecimiento del entorno digital de una organización.

Objetivos Específicos

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías de pruebas de penetración y técnicas de intrusión.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Generar recomendaciones y conclusiones que permitan tomarse como referencia para el fortalecimiento de un entorno digital.

Desarrollo del Trabajo

Identificar la Legislación Relacionada con Delitos Informáticos en Colombia, Resaltando sus Principales Características.

Dentro del Margen Legal en Colombia Sobre Delitos Informáticos y Protección de Datos Personales Redacte con sus Propias Palabras que Legislación "Leyes, Decretos" Existen Actualmente y las Características Principales de Cada Ley.

Tabla 1

Legislación Relacionada con Delitos Informáticos en Colombia

Legislación	Descripción	Características Principales
Ley 1273 de 2009	Ley de Delitos Informáticos	Modificó el Código Penal colombiano (Ley 599 de 2000) tipificando conductas con el fin de incluir delitos específicos relacionados con el uso de tecnologías de la información como el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales, la suplantación de sitios web para capturar datos personales, el hurto por medios informáticos y semejantes, la transferencia no consentida de activos. Establece penas de prisión y multas para quienes incurran en estos delitos.
Ley 1581 de 2012	Ley de Protección de Datos Personales	Regula el tratamiento de datos personales en Colombia estableciendo principios como la legalidad, la finalidad, la libertad, la veracidad o calidad, la transparencia, el acceso y circulación restringida, la seguridad y la confidencialidad en el manejo de datos. Otorga derechos a los titulares de los datos como el acceso, la cancelación, la oposición y la rectificación. Crea el Registro Nacional de Bases de Datos (RNBD). Se utiliza con el fin de proteger la información personal que es manipulada por terceros o empresas, para evitar el uso malintencionado de esta.

Decreto 1377 de 2013	Reglamentación de la Ley 1581 de 2012	Desarrolla las disposiciones de la Ley 1581 de 2012 estableciendo los requisitos y procedimientos para el tratamiento de datos personales. Define las obligaciones de los responsables y encargados del tratamiento de datos. Regula la transferencia internacional de datos personales. Da una guía más específica de cómo desarrollar la ley previamente escrita.
Ley 1955 de 2019	Plan Nacional de Desarrollo 2018-2022	Incluye disposiciones relacionadas con la transformación digital y la seguridad cibernética promoviendo la adopción de medidas para proteger la infraestructura crítica cibernética. Fomenta la cooperación entre el sector público y privado en materia de seguridad cibernética. Busca fortalecer la seguridad cibernética del país frente a los constantes ataques a la seguridad de la información.

Nota: Legislación, descripción y características principales.

Reconocer y Describir el Ejercicio de Pentesting, sus Etapas y Herramientas Utilizadas.

En el Mundo de la Ciberseguridad Existen Procesos Definidos Para Poder Ejecutar de Forma Organizada lo que se Conoce Como Pruebas de Penetración o Pentesting; Usted Como Futuro Experto Deberá Redactar con sus Palabras y Definir Cada Una de las Etapas del Pentesting, Dentro de la Definición Incorporará un Ejemplo de Una Herramienta que se Utilice Para Cada Una de las Etapas del Pentesting.

Tabla 2

Etapas del Pentesting

Etapa del Pentesting	Descripción	Herramienta Ejemplo
Planificación	Se define el alcance del pentesting, los sistemas a evaluar, los objetivos específicos y las reglas de compromiso. Se establece un acuerdo entre el pentester y la organización objetivo, definiendo los límites de la prueba.	Documentos de planificación personalizados, plantillas de alcance de pentesting.
Reconocimiento	Se recopila información sobre el objetivo con el fin de entender su infraestructura de red, sistemas operativos, aplicaciones web, usuarios y posibles vulnerabilidades. Se pueden usar técnicas de recolección pasiva (sin interacción directa) o activa (interactuando con el objetivo).	Nmap: Permite el escaneo de redes para identificar puertos abiertos y descubrir servicios disponibles. Sublist3r: Script en Python que permite enumerar subdominios en sitios web.

Escaneo y Análisis	Se utilizan herramientas para mapear la red y obtener detalles técnicos más profundos de los sistemas identificados en el reconocimiento, como versiones de software y sistemas operativos. Se utilizan herramientas de escaneo de vulnerabilidades para identificar fallos de seguridad conocidos. Una vez recopilada la información, se analizan las posibles vulnerabilidades presentes en el sistema objetivo.	Nessus Essentials: Identifica vulnerabilidades en sistemas y configuraciones. OpenVAS: escaneo de vulnerabilidades.
Explotación	El pentester busca explotar las vulnerabilidades identificadas para lograr el ingreso no autorizado a sistemas, aplicaciones o información. Con el fin de demostrar qué tan vulnerables son los sistemas a ataques reales, se utilizan técnicas de hacking ético como inyección SQL, cross-site scripting (XSS) o desbordamiento de búfer.	Metasploit Framework: Utilizada para desarrollar y ejecutar exploits contra sistemas vulnerables.
Post-explotación y Mantenimiento del Acceso	Después de obtener acceso, el pentester evalúa el impacto del ataque y la capacidad del atacante para mantener el acceso al sistema. Se busca información confidencial, se elevan privilegios y se exploran las posibilidades de movimientos laterales dentro de la red. Se establecen puertas traseras o persistencia para acceder a los sistemas en caso de que se cierre la vulnerabilidad explotada. Esto simula escenarios de intrusos que buscan acceso prolongado.	Cobalt Strike: Utilizada para simular persistencia y explotación avanzada. PowerSploit: Utilizada para tareas de post-explotación en entornos Windows.

Análisis y Reporte	El pentester documenta detalladamente todos los resultados y los hallazgos del pentesting, presentando un informe detallado para los responsables de la organización objetivo. Este informe debe describir el impacto potencial de las vulnerabilidades detectadas, los exploits utilizados, las pruebas realizadas y recomendaciones para mitigarlas y mejorar la seguridad.	Dradis Framework: Utilizada para organizar y presentar reportes de forma profesional.

Nota: Etapas del Pentesting, descripción y herramienta ejemplo.

Identificar, Reconocer y Explicar Herramientas Necesarias Para el Desarrollo de Ejercicios de Seguridad Informática, Explicando sus Capacidades, Funcionamiento y Utilidad Para el Ejercicio.

Las Herramientas de Ciberseguridad son de Vital Importancia, Además que Existe un Gran Abanico de Posibilidades de Herramientas Existentes y Software Especializado para Desarrollar Herramientas Propias. Usted Como Futuro Experto Debe Definir y Explicar las Siguientes Herramientas (Metasploit, Nmap y Openvas) y Servicios en Línea (ExploitDB y CVE).

Tabla 3

Herramientas y servicios en línea para ejercicios de seguridad informática

Herramienta/Servicio	Capacidades	Funcionamiento	Utilidad
Metasploit	Proporciona una plataforma para desarrollar y ejecutar código de exploits contra sistemas remotos. Incluye una amplia base de datos de exploits para diversas vulnerabilidades. Permite automatizar tareas de pentesting, desde el escaneo de vulnerabilidades hasta la post-explotación.	Funciona a través de módulos que contienen código para exploits, payloads (código malicioso que se ejecuta en el sistema objetivo) y auxiliares (herramientas para tareas específicas). El pentester selecciona un exploit, configura las opciones necesarias y ejecuta el ataque contra el sistema objetivo. Después de obtener acceso, permite realizar tareas de post-explotación, como recopilación de información y escalada de privilegios.	Herramienta esencial para pentesters y profesionales de seguridad que necesitan simular ataques cibernéticos y evaluar la seguridad de sistemas informáticos. Permite identificar y explotar vulnerabilidades de forma controlada, lo que ayuda a las organizaciones a fortalecer su seguridad.

Nmap	Herramienta de escaneo de puertos y mapeo de redes que permite descubrir hosts y servicios en una red. Puede identificar sistemas operativos, versiones de software y firewalls. Ofrece diversas técnicas de escaneo, desde escaneo de puertos TCP/UDP hasta detección de sistemas operativos remotos.	Envía paquetes de datos a los sistemas objetivo y analiza las respuestas para determinar qué puertos están abiertos, qué servicios se están ejecutando y qué sistemas operativos se están utilizando. Permite personalizar los escaneos mediante diversas opciones y scripts.	Herramienta fundamental para el reconocimiento de redes y la identificación de posibles vectores de ataque. Ayuda a los profesionales de seguridad a comprender la topología de una red y a identificar posibles vulnerabilidades.
OpenVAS	Escáner de vulnerabilidades de código abierto que permite identificar fallos de seguridad en sistemas y aplicaciones. Utiliza una base de datos de vulnerabilidades conocida como NVT (Network Vulnerability Tests). Puede generar informes detallados sobre las vulnerabilidades encontradas.	Funciona mediante de la ejecución de NVT's, que son scripts los cuales revisan por la presencia de vulnerabilidades en el sistema en cuestión. Los resultados son presentados al usuario en reportes, los cuales priorizan las vulnerabilidades encontradas según su nivel de criticidad.	Herramienta importante para la gestión de vulnerabilidades y la evaluación continua de la seguridad. Permite a las organizaciones identificar y corregir fallos de seguridad antes de que sean explotados por atacantes.
ExploitDB	Base de datos en línea de exploits y vulnerabilidades. Contiene una gran cantidad de código de exploits para diversas vulnerabilidades, tanto conocidas como de día cero (zero-day).	Funciona como un repositorio donde los investigadores de seguridad y los pentesters pueden compartir y descargar exploits.	Recurso valioso para los pentesters y los investigadores de seguridad que necesitan encontrar exploits para vulnerabilidades específicas. Permite comprender como explotan los atacantes diferentes vulnerabilidades.

CVE	Sistema de numeración estandarizado para vulnerabilidades y exposiciones de seguridad informática. Proporciona un identificador único para cada vulnerabilidad conocida.	Asigna un número de identificación único a cada vulnerabilidad que se hace pública. Este número se utiliza para hacer referencia a la vulnerabilidad en bases de datos de vulnerabilidades, alertas de seguridad y otras fuentes de información.	Estándar importante para la gestión de vulnerabilidades y la comunicación entre profesionales de seguridad. Permite a las organizaciones realizar un seguimiento de las vulnerabilidades que afectan a sus sistemas y aplicaciones.

Nota: Herramienta, Capacidad, Funcionamiento y Utilidad.

Implementar Escenarios Tecnológicos Controlados Para el Desarrollo de Ejercicios de Pentesting Funcionales

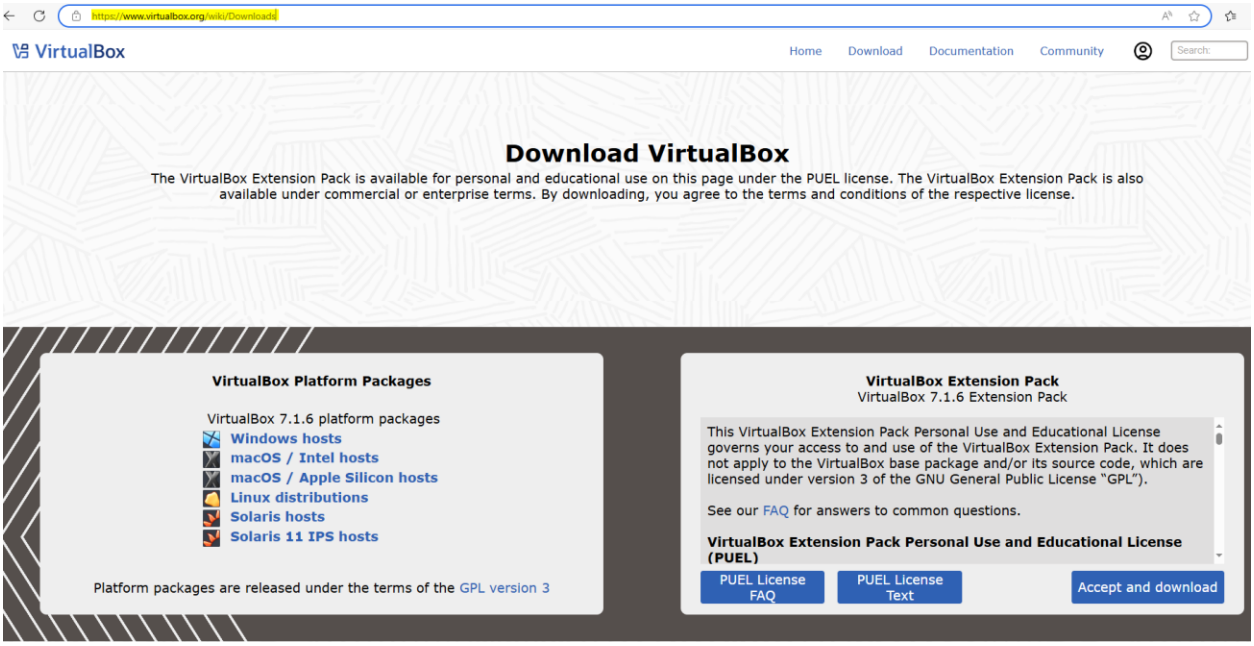
Para Finalizar Esta Actividad es Importante que Usted Reconozca, Analice y Configure "banco de trabajo" lo Solicitado en el Anexo 1 – Escenario 1 Sobre el Cual Deberá Trabajar Actividades que Contienen un Alto Grado de Tecnicidad. Lo Solicitado en el Anexo 1 – Escenario 1 es lo Siguiente:

Paso A: Descargar la herramienta virtualizadora "VirtualBox" en su última versión.

Para descargar la última versión de la herramienta virtualizadora "VirtualBox" se accede a la URL https://www.virtualbox.org/wiki/Downloads, se selecciona el paquete según la plataforma, en este caso se selecciona "Windows hosts" y se realiza la descarga del archivo VirtualBox-7.1.6-167084-Win.exe desde el siguiente enlace https://download.virtualbox.org/virtualbox/7.1.6/VirtualBox-7.1.6-167084-Win.exe

Figura 1

Descarga de la última versión de VirtualBox

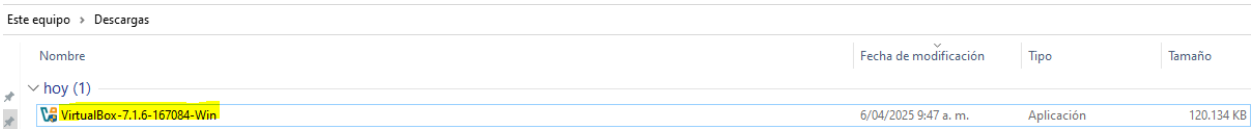


Nota: *URL para la descarga de la última versión de VirtualBox.*

El archivo VirtualBox-7.1.6-167084-Win.exe se descarga en el equipo.

Figura 2

Última versión de VirtualBox descargada

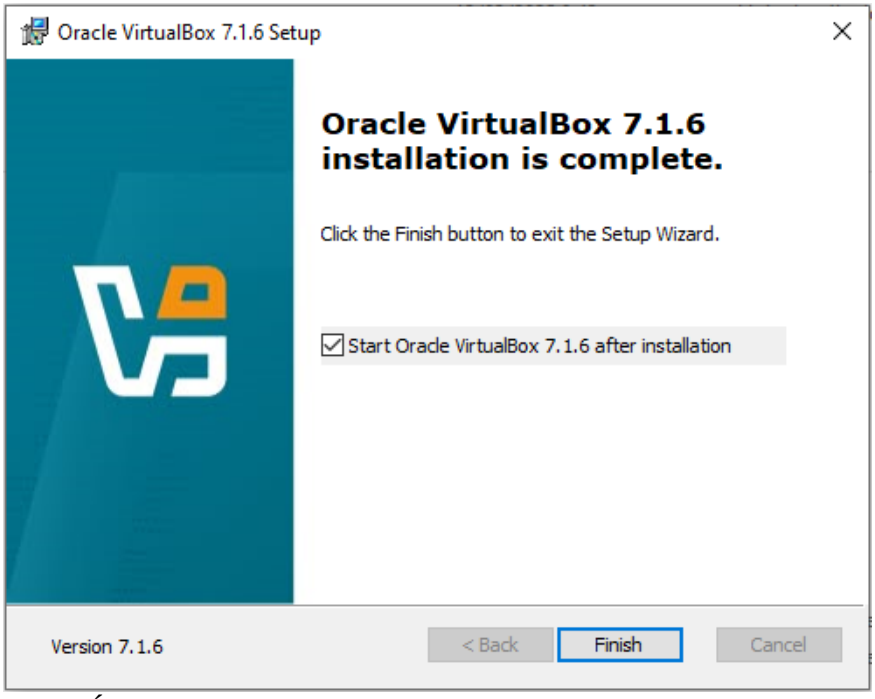


Nota: *Archivo ejecutable con la última versión de VirtualBox descargada.*

Se ejecuta el archivo VirtualBox-7.1.6-167084-Win.exe y se realiza la instalación de la última versión de VirtualBox en el equipo.

Figura 3

Última versión de VirtualBox instalada



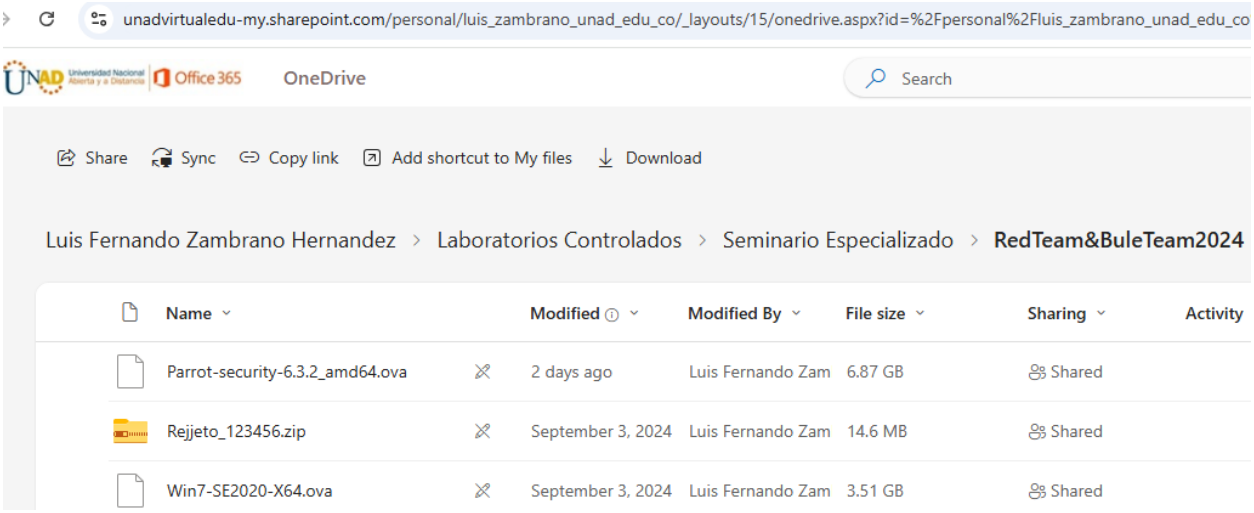
Nota: *Última versión de VirtualBox instalada.*

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad ingrese al enlace: RedTeam&BuleTeam2024, el cual contiene lo requerido para el montaje del banco de trabajo, las imágenes en formato *.OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un sistema operativo Windows y un sistema operativo Kali Linux.

Se ingresa a la carpeta compartida ejecuta RedTeam&BuleTeam2024 la cual contiene tres (3) archivos para el montaje del banco de trabajo.

Figura 4

Carpeta RedTeam&BuleTeam2024

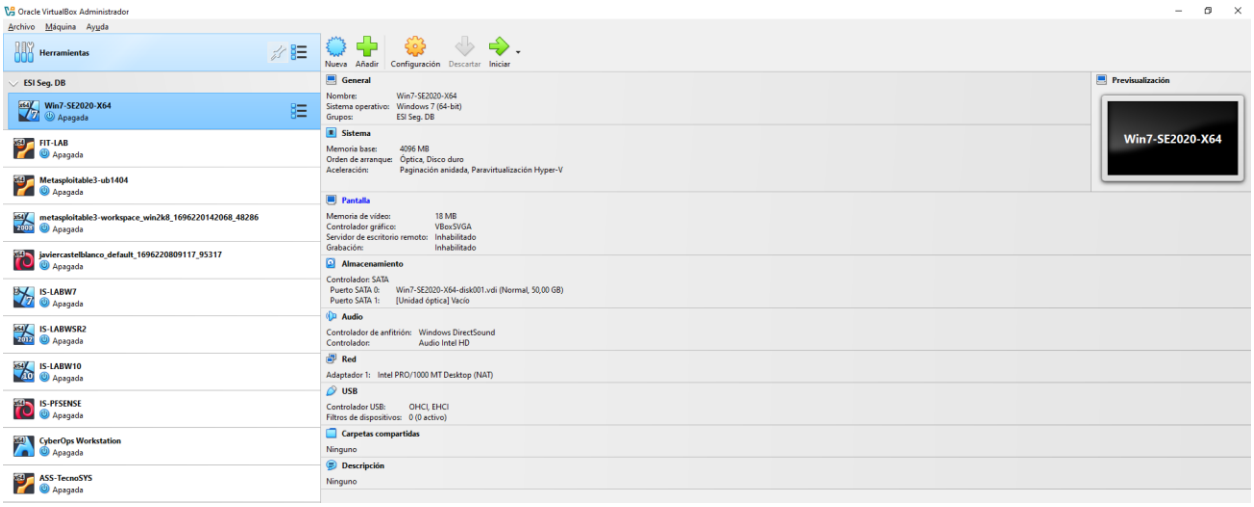


Nota: *Archivos dentro de la carpeta RedTeam&BuleTeam2024.*

Se ejecuta el archivo Win7-SE2020-X64.ova y se realiza la importación del servicio virtualizado o de la máquina virtual Win7-SE2020-X64 en VirtualBox.

Figura 5

Importación de la máquina virtual Win7-SE2020-X64 en VirtualBox

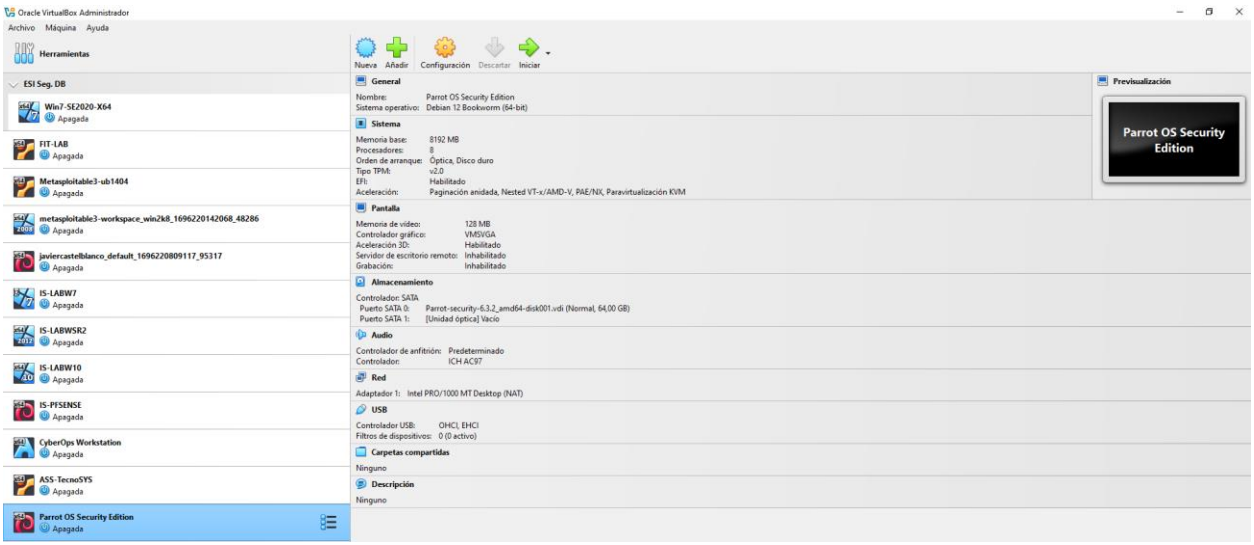


Nota: *Máquina virtual Win7-SE2020-X64 importada en VirtualBox.*

Se ejecuta el archivo Parrot-security-6.3.2_amd64.ova y se realiza la importación del servicio virtualizado o de la máquina virtual Parrot-security-6.3.2_amd64 en VirtualBox.

Figura 6

Importación de la máquina virtual Parrot OS Security Edition en VirtualBox

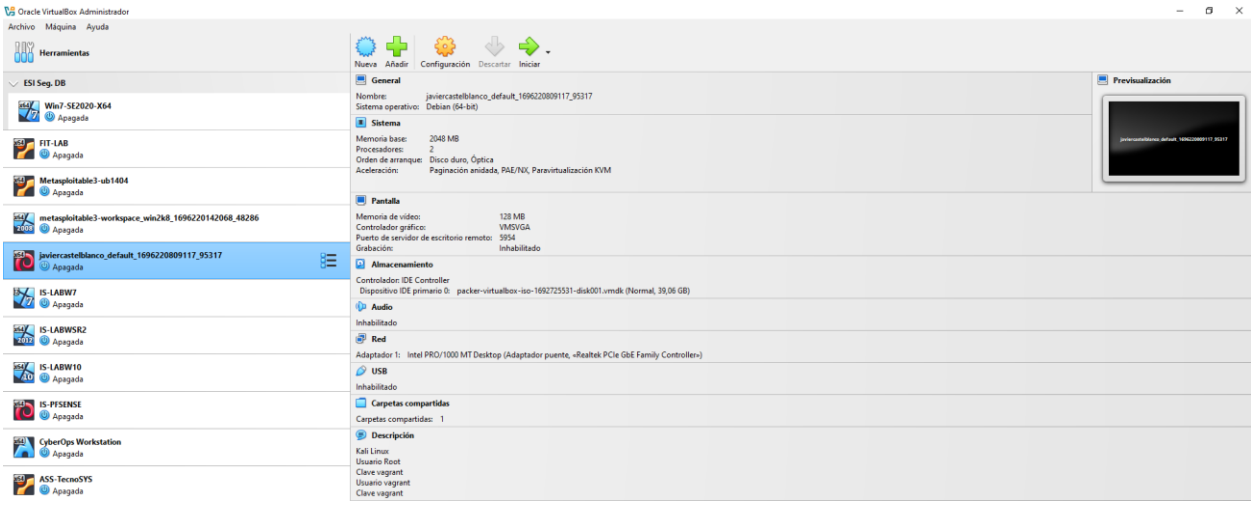


Nota: *Máquina virtual Parrot OS Security Edition importada en VirtualBox.*

Se cuenta con una máquina virtual Kali Linux instalada en VirtualBox.

Figura 7

Máquina virtual Kali Linux en VirtualBox



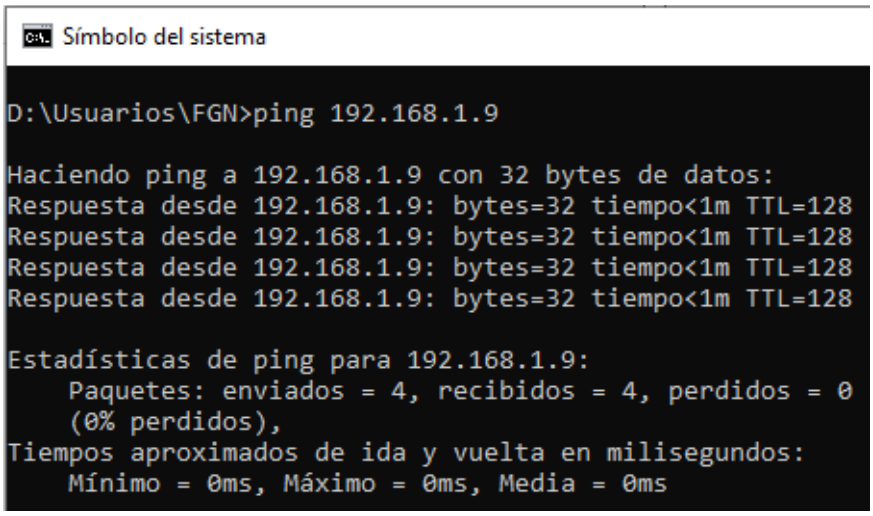
Nota: *Máquina virtual Kali Linux instalada en VirtualBox.*

Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Se realiza la validación de la comunicación entre la máquina física (equipo Host) que tiene la dirección IP 192.168.1.8 con la máquina virtual Win7-SE2020-X64 instalada en VirtualBox que tiene la dirección IP 192.168.1.9 mediante el comando ping 192.168.1.9

Figura 8

Ping desde el equipo host hacia la máquina virtual Win7-SE2020-X64

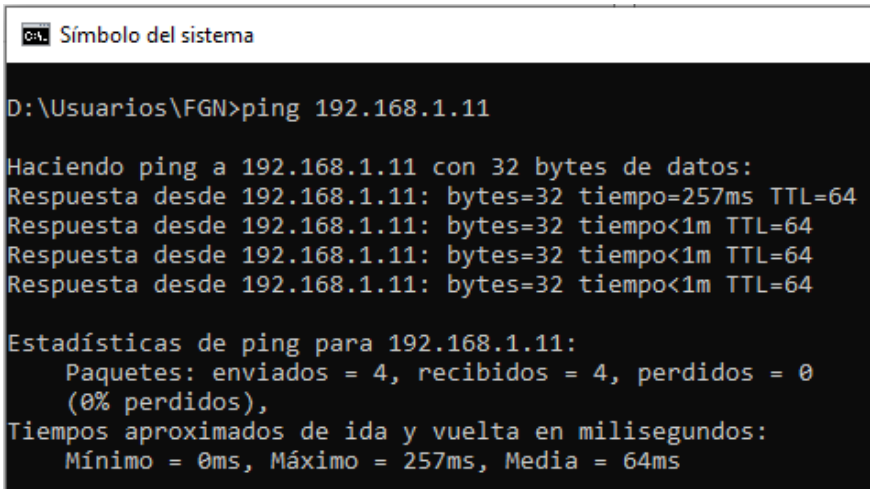


Nota: *Comunicación entre la máquina física (equipo Host) con la máquina virtual Win7-SE2020-X64.*

Se realiza la validación de la comunicación entre la máquina física (equipo Host) que tiene la dirección IP 192.168.1.8 con la máquina virtual Kali Linux instalada en VirtualBox que tiene la dirección IP 192.168.1.11 mediante el comando ping 192.168.1.11

Figura 9

Ping desde el equipo host hacia la máquina virtual Kali Linux

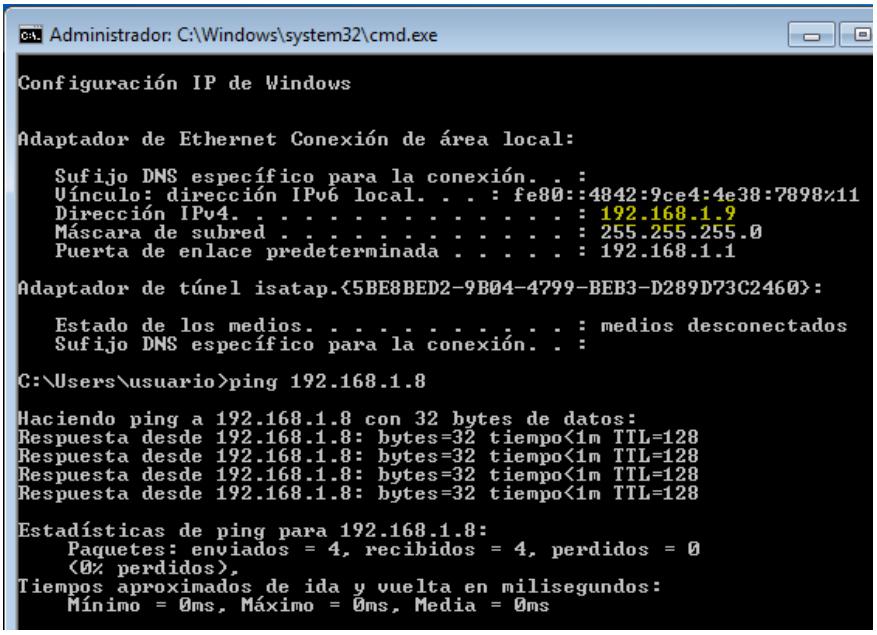


Nota: *Comunicación entre la máquina física (equipo Host) con la máquina virtual Kali Linux.*

Se realiza la validación de la comunicación entre la máquina virtual Win7-SE2020-X64 instalada en VirtualBox que tiene la dirección IP 192.168.1.9 con la máquina física (equipo Host) que tiene la dirección IP 192.168.1.8 mediante el comando ping 192.168.1.8

Figura 10

Ping desde la máquina virtual Win7-SE2020-X64 hacia el equipo host

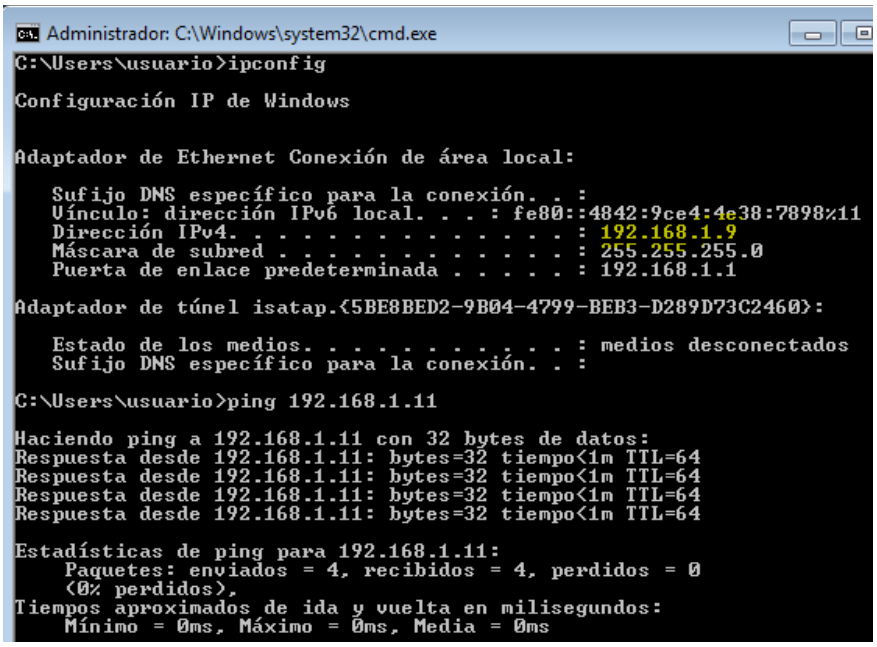


Nota: *Comunicación entre la máquina virtual Win7-SE2020-X64 con la máquina física (equipo Host).*

Se realiza la validación de la comunicación entre la máquina virtual Win7-SE2020-X64 instalada en VirtualBox que tiene la dirección IP 192.168.1.9 con la máquina virtual Kali Linux instalada en VirtualBox que tiene la dirección IP 192.168.1.11 mediante el comando ping 192.168.1.11

Figura 11

Ping desde la máquina virtual Win7-SE2020-X64 hacia la máquina virtual Kali Linux

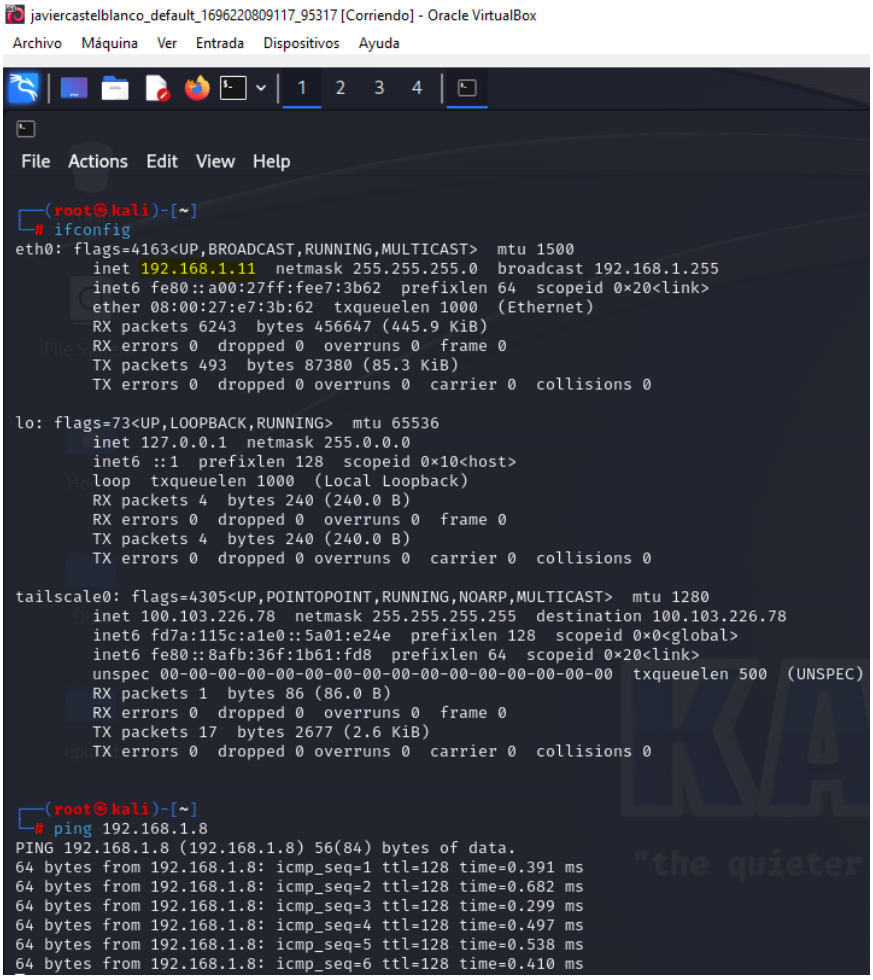


Nota: *Comunicación entre la máquina virtual Win7-SE2020-X64 con la máquina virtual Kali Linux.*

Se realiza la validación de la comunicación entre la máquina virtual Kali Linux instalada en VirtualBox que tiene la dirección IP 192.168.1.11 con la máquina física (equipo Host) que tiene la dirección IP 192.168.1.8 mediante el comando ping 192.168.1.8

Figura 12

Ping desde la máquina virtual Kali Linux hacia el equipo host

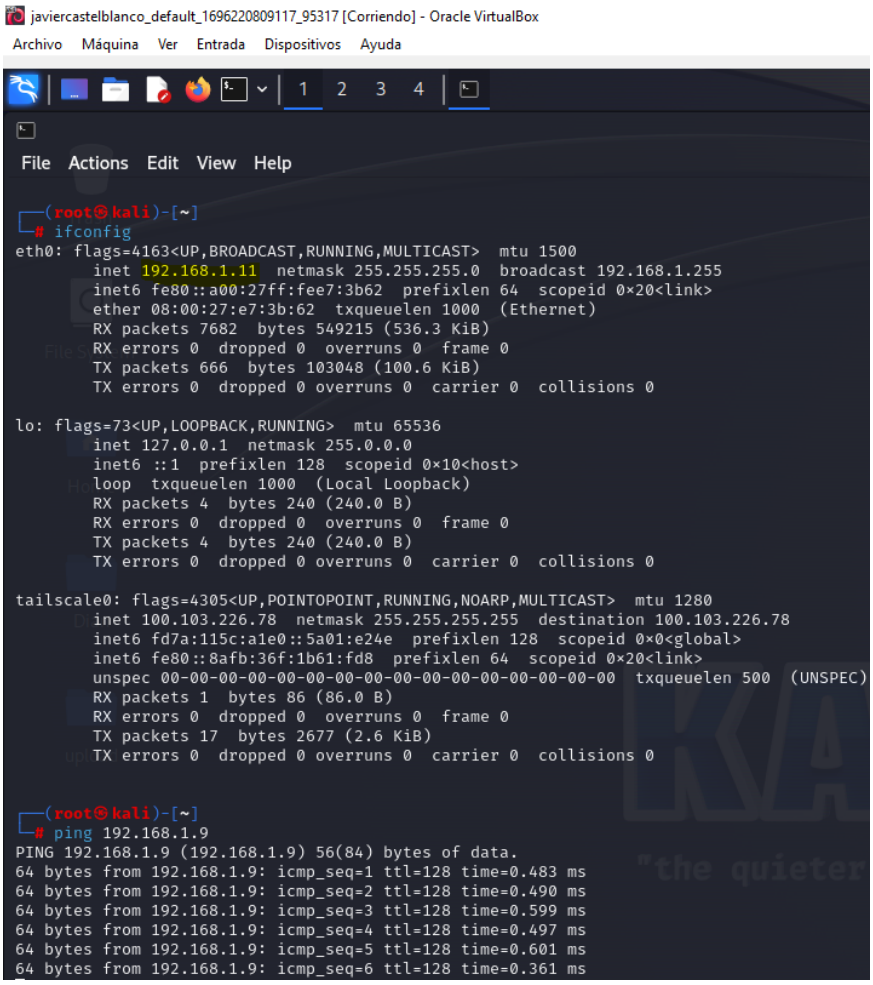


Nota: *Comunicación entre la máquina virtual Win7-SE2020-X64 con la máquina física (equipo Host).*

Se realiza la validación de la comunicación entre la máquina virtual Kali Linux instalada en VirtualBox que tiene la dirección IP 192.168.1.11 con la máquina virtual Win7-SE2020-X64 instalada en VirtualBox que tiene la dirección IP 192.168.1.9 mediante el comando ping 192.168.1.9

Figura 13

Ping desde la máquina virtual Kali Linux hacia la máquina virtual Win7-SE2020-X64



Nota: *Comunicación entre la máquina virtual Win7-SE2020-X64 con la máquina virtual Kali Linux.*

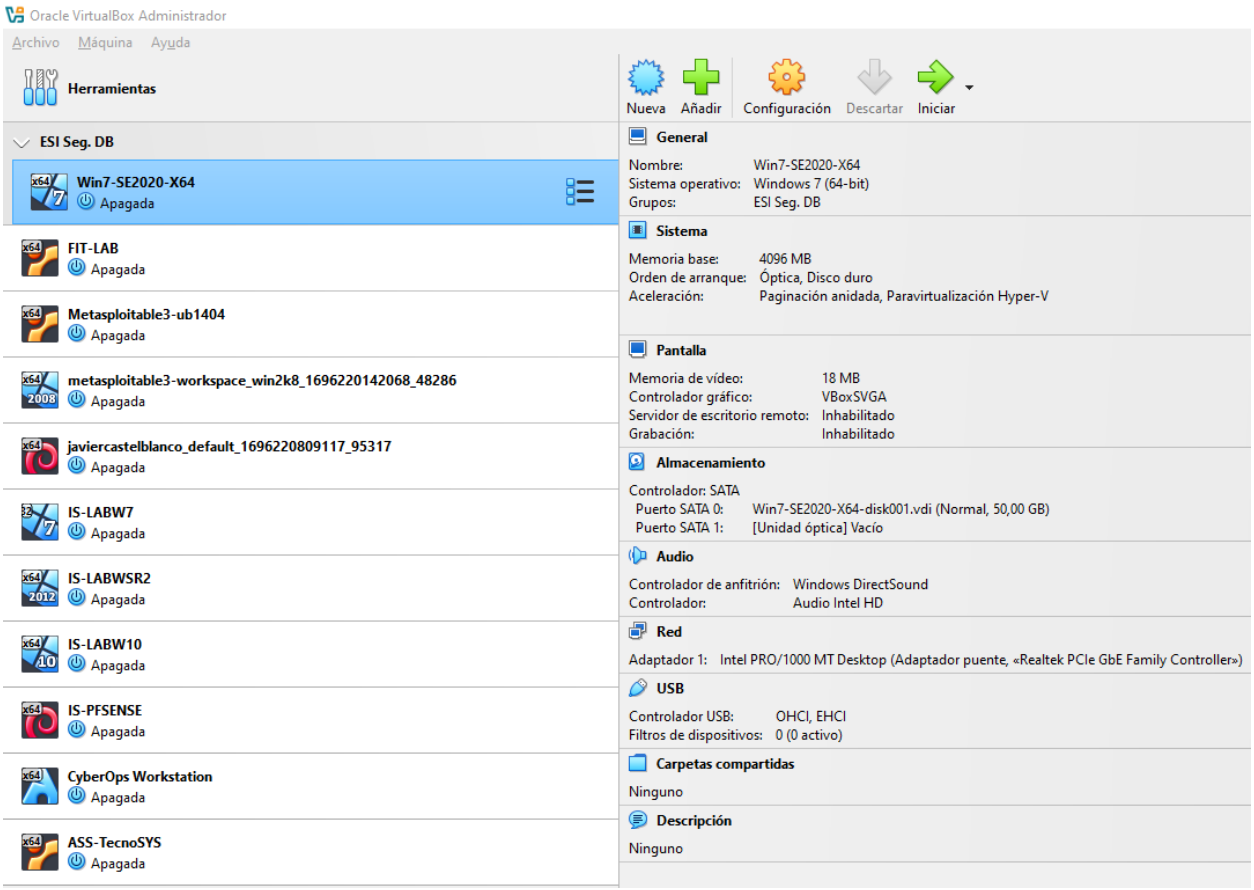
Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado "características técnicas de hardware".

El montaje del banco de trabajo se realizó en VirtualBox y consta de la máquina virtual Win7-SE2020-X64 y de la máquina virtual Kali Linux.

Las siguientes son las características técnicas de hardware de la máquina virtual Win7-SE2020-X64:

Figura 14

Características técnicas de hardware de la máquina virtual Win7-SE2020-X64

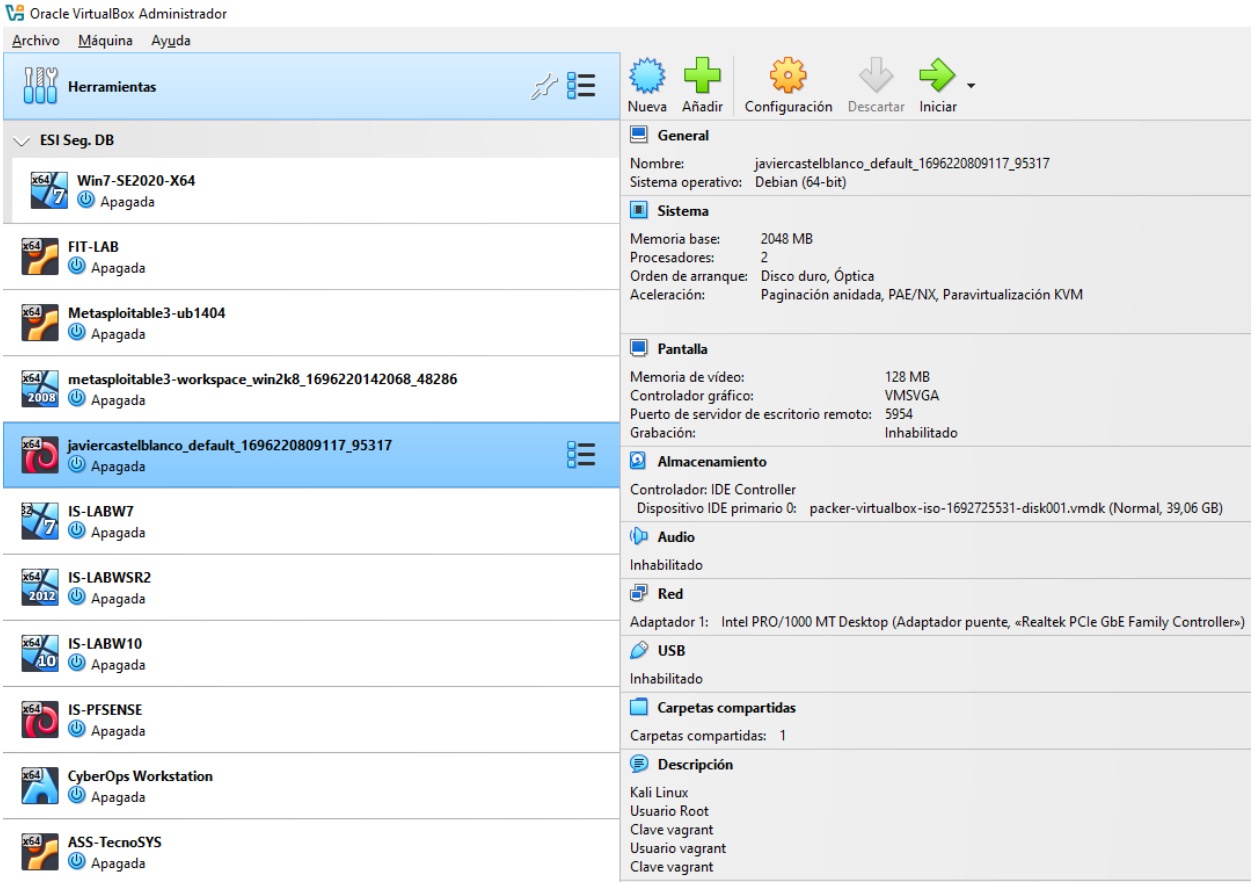


Nota: *General, Sistema, Pantalla, Almacenamiento, Audio, Red, USB, Carpetas compartidas y Descripción de las características técnicas de hardware de la máquina virtual Win7-SE2020-X64.*

Las siguientes son las características técnicas de hardware de la máquina virtual Kali Linux:

Figura 15

Características técnicas de hardware de la máquina virtual Kali Linux



Nota: *General, Sistema, Pantalla, Almacenamiento, Audio, Red, USB, Carpetas compartidas y Descripción de las características técnicas de hardware de la máquina virtual Kali Linux.*

Analizar los Anexos Propuestos Identificando Adecuadamente Posibles Situaciones no Legales o no Éticas, Argumentando su Respuesta Adecuadamente

Una Vez Leído el Anexo 2 – Escenario 2 y el Anexo 3 – Acuerdo, ¿Usted Logra Evidenciar Algún Proceso Ilegal y No Ético Que se Esté Estipulando en Dicho Acuerdo? Deberá Argumentar su Respuesta y Señalar los Fragmentos Ilegales del Anexo 3 - Acuerdo en Caso de Existir Alguna Irregularidad

Tras una revisión minuciosa del Anexo 2 - Escenario 2 y el Anexo 3 - Acuerdo de Confidencialidad, es innegable que el acuerdo contiene varias estipulaciones que no solo rayan en la falta de ética, sino que directamente contravienen principios legales fundamentales. La raíz del problema se encuentra en la intención, aparentemente deliberada, de blindar a CyberFort Technologies de cualquier responsabilidad por actos ilícitos, a la vez que se impone a la parte receptora (el estudiante/candidato) la obligación de guardar silencio sobre estos.

A continuación, se argumenta esta afirmación y se señalan los fragmentos específicos del Anexo 3 que fundamentan dicha ilegalidad:

Argumentación de la Ilegalidad y Falta de Ética

El Anexo 2 - Escenario 2, nos plantea un escenario donde la propia gerencia de CyberFort Technologies es consciente de que el contrato y los acuerdos de confidencialidad fueron elaborados por un abogado despedido por detectar "algunos procesos ilícitos" y, aun así, decide seguir adelante sin revisarlos adecuadamente. Esta actitud inicial ya levanta serias sospechas sobre la ética profesional de la organización al no asegurar la legalidad y ética de sus procesos de contratación y su posible predisposición a tolerar, o incluso encubrir, actividades cuestionables.

Pero es en el Anexo 3 - Acuerdo de Confidencialidad donde se encuentran las cláusulas que confirman estas sospechas. Varias de ellas buscan explícitamente que la parte receptora (el estudiante/candidato) se convierta en cómplice pasivo de potenciales ilegalidades como no denunciar actividades ilícitas, lo cual es una clara violación de la ley.

Tabla 4

Fragmentos Ilegales del Anexo 3 - Acuerdo de Confidencialidad

Cláusula	Descripción	Ilegalidad / Falta de Ética
Segunda, numeral 2	"datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'."	La mención explícita de actividades ilegales como "chuzadas" o "accesos abusivos" es sumamente preocupante. Parece una admisión tácita de que la empresa podría estar involucrada en estas prácticas, y que el acuerdo busca garantizar el silencio de los empleados al respecto.
Cuarta, numeral 3	"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros".	Esta cláusula es abiertamente ilegal. Impedir que alguien denuncie un delito es obstrucción a la justicia. Además, es completamente contrario a la ética profesional de cualquier persona, especialmente en el campo de la seguridad de la información, donde la denuncia de actividades ilícitas es fundamental.
Cuarta, numeral 4	"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas".	Similar al punto anterior, esta cláusula también busca impedir la denuncia de actividades ilegales, lo cual es contrario a la ley.

Octava	"En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies".	Esta cláusula es ilegal ya que ninguna persona puede ser obligada a renunciar a su derecho a denunciar un delito. Además, exime a la empresa de cualquier responsabilidad penal, lo cual es contrario a la ley. Si un empleado tiene conocimiento de actividades ilegales dentro de la empresa, tiene el derecho e incluso el deber de denunciarlas ante las autoridades competentes.

Nota: Cláusula, descripción e ilegalidad o falta de ética.

Analizar los Anexos e Identificar Posibles Vulneraciones a la Ley 1273, Justificando por qué Adecuadamente

Si la Respuesta es Afirmativa y Usted Encontró Algún Proceso Ilegal en el Anexo 3 – Acuerdo, Deberá Mencionar qué Artículos de la Ley 1273 se Podrían Vulnerar en Dicho Acuerdo y Especificar Porqué Vulnera Artículos de La Ley 1273

Es crucial entender que la Ley 1273 busca proteger la confidencialidad, la disponibilidad y la integridad de la información, así como sancionar las conductas que atenten contra los sistemas informáticos. El Acuerdo de Confidencialidad, al incluir cláusulas que obligan al empleado a guardar silencio sobre actividades ilegales, podría facilitar o incluso promover la comisión de varios de estos delitos, lo cual es una clara obstrucción a la aplicación de esta ley.

Además, al mencionar explícitamente "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos", el acuerdo parece prever o incluso contemplar la posibilidad de que se cometan delitos informáticos.

Es fundamental tener en cuenta que un acuerdo no puede estar por encima de la ley. Cualquier cláusula que obligue a una persona a no denunciar un delito es nula y carece de validez legal.

Como se mencionó anteriormente, el Anexo 3 - Acuerdo contiene procesos ilegales. A continuación, se especifican algunos artículos de la Ley 1273 de 2008 (Ley de Delitos Informáticos) que podrían vulnerarse con dicho acuerdo, y se especifica el porqué de su vulneración:

Tabla 5
Artículos de la Ley 1273 de 2008 que podrían vulnerarse

Artículo	Descripción	Por qué se vulnera
Artículo 269A. Acceso abusivo a un sistema informático	"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."	La cláusula que menciona "datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'" podría interpretarse como una aceptación o incluso una instrucción para obtener información de manera ilegal. Si el acuerdo implica que el empleado tenga acceso a este tipo de información obtenida ilícitamente o se le exige no denunciarlo, se estaría promoviendo o encubriendo un delito tipificado en este artículo.
Artículo 269F. Violación de datos personales	"El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes."	Si en el desarrollo de las actividades descritas en el acuerdo se llegaran a manejar datos personales de manera ilegal (obtención, divulgación, etc.), se estaría incurriendo en este delito. La obligación de no denunciar información ilegal (Cláusula Cuarta, numeral 4) agrava la situación, pues impide que se persiga este delito.
Artículo 269G. Suplantación de sitio web para capturar datos personales	"El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave."	Aunque no es tan directo como los anteriores, este artículo es relevante en el contexto de ciberseguridad. Si las "actividades ilegales" que el empleado se compromete a no denunciar involucran la suplantación de sitios web o la utilización de software malicioso para capturar datos, se estaría facilitando la comisión de este delito.

Nota: Artículo, descripción y porqué se vulnera.

Analizar una Propuesta Laboral Identificando Aspectos Éticos y Argumentando la Decisión de Aplicar o no a Dicha Propuesta

Existiendo Procesos Poco Confiables en el Anexo 3 – Acuerdo, Usted Como Experto en Ciberseguridad ¿Aplicaría a Este Trabajo en Cyberfort Technologies, Donde la Organización Dispone de un Sueldo de $15.000.000 de Pesos Colombianos Mensuales y Contrato Vitalicio? Debe Argumentar su Respuesta ya Sea Afirmativa o Negativa y Tener en Cuenta en la Argumentación que Dispone COPNIA en su Código de Ética Para Ingenieros

Esta es una pregunta compleja que requiere una cuidadosa consideración de los factores éticos, legales y profesionales en juego. Como experto en ciberseguridad, **no aplicaría a este trabajo** en CyberFort Technologies, a pesar del atractivo salario y el contrato vitalicio, mi compromiso con la ética profesional, la legalidad y la responsabilidad social me impediría aceptar un trabajo que implique la participación o el encubrimiento de actividades ilícitas.

La siguiente es la argumentación de mi respuesta teniendo como referencia el Código de Ética para Ingenieros del Consejo Profesional Nacional de Ingeniería - COPNIA:

1. **Prioridad de la Ética Profesional:** El Código de Ética para Ingenieros del COPNIA establece claramente la primacía de la ética en el ejercicio de la profesión. Los ingenieros deben actuar con integridad, honestidad y responsabilidad, priorizando el bienestar público y el cumplimiento de la ley sobre el beneficio personal o económico.
2. **Implicaciones Legales y Éticas del Acuerdo:** Como se analizó anteriormente, el Anexo 3 - Acuerdo contiene cláusulas que promueven la ilegalidad y la falta de ética. Aceptar un trabajo que requiera la firma de dicho acuerdo me convertiría en cómplice de actividades ilícitas y violaría mis principios éticos como profesional de la ciberseguridad.

3. **Riesgos Profesionales y Personales:** Involucrarme en actividades ilegales, incluso bajo la promesa de inmunidad, conlleva graves riesgos profesionales y personales. Podría enfrentar sanciones legales, perder mi licencia profesional y dañar irreparablemente mi reputación. Además, estaría contribuyendo a un ambiente de trabajo corrupto y poco ético, lo cual va en contra de mi responsabilidad social como ingeniero.
4. **Responsabilidad del Ingeniero en Ciberseguridad:** Los profesionales de la ciberseguridad tienen la responsabilidad de proteger la información y los sistemas informáticos, así como de promover la seguridad y la confianza en el entorno digital. Aceptar un trabajo en una organización que participa en actividades ilícitas va en contra de esta responsabilidad y socava la integridad de la profesión.
5. **Alternativas Profesionales:** Aunque el salario y el contrato vitalicio pueden ser atractivos, existen muchas otras oportunidades profesionales en el campo de la ciberseguridad donde puedo ejercer mi profesión de manera ética y legal. A largo plazo, mantener mi integridad y reputación profesional es mucho más valioso que cualquier beneficio económico a corto plazo.

Consideraciones del Código de Ética del COPNIA

El Código de Ética del COPNIA enfatiza los siguientes principios, que serían violados al aceptar el trabajo en CyberFort Technologies:

- **Competencia Profesional:** Mantener altos estándares de competencia y ética en el ejercicio de la profesión.
- **Integridad:** Actuar con honestidad y transparencia en todas las actividades profesionales.
- **Legalidad:** Cumplir con las leyes y regulaciones vigentes.
- **Responsabilidad Social:** Contribuir al bienestar público y al desarrollo sostenible.

Analizar el Caso de “Ciber espionaje y Ética en Cyberfort Technologies”, Identificando Adecuadamente las Implicaciones Éticas y Legales que Pudo Generar

Deberá Analizar el Caso Problema “Ciber espionaje y Ética en Cyberfort Technologies” (Anexo 7 - Escenario 2), Redactar su Punto de Vista Teniendo en Cuenta las Implicaciones Legales y Éticas Que Allí se Pudieron Generar y Dar Respuesta a los Interrogantes

Punto de Vista sobre el Caso "Ciber espionaje y Ética en CyberFort Technologies"

El caso de CyberFort Technologies constituye un ejemplo alarmante de cómo los límites éticos en el ámbito de la seguridad cibernética pueden volverse peligrosamente difusos. Estas compañías deberían ser los custodios de nuestra información, quienes garantizan nuestra protección frente a las amenazas digitales. Sin embargo, este caso muestra una situación donde la empresa, o al menos ciertos integrantes de su equipo, aprovechan su posición de confianza para vigilar indebidamente a un cliente y, aún peor, obtener beneficios económicos mediante el uso indebido de datos robados.

Lo que resulta especialmente preocupante es la argumentación que buscan utilizar para justificar sus acciones, esa noción de que actúan con el propósito de "garantizar la seguridad" del cliente. Este razonamiento es claramente retorcido, dado que existe una enorme distancia entre fortalecer la seguridad de un cliente con su autorización y supervisarlo sin su conocimiento. La ausencia de consentimiento, en mi perspectiva, es el factor determinante que transforma esta conducta en ciber espionaje y en una seria infracción de los principios éticos profesionales.

Por otro lado, la comercialización de la información en redes clandestinas como la Darknet y su venta a competidores representa una deslealtad absoluta hacia la confianza depositada en CyberFort Technologies. Este acto no solo perjudica directamente al cliente afectado, sino que también socava la credibilidad de toda la industria de la ciberseguridad.

¿Cómo podríamos confiar en estas compañías si están dispuestas a traicionarnos de una manera tan descarada?

¿Hasta qué Punto las Empresas de Ciberseguridad Deben Tener Acceso a Información Sensible de sus Clientes Durante una Auditoría de Seguridad, y Cómo se Puede Garantizar que Este Acceso no Sea Explotado de Manera Indebida?

Creo que las empresas de ciberseguridad *necesitan* tener acceso a información sensible de sus clientes durante una auditoría. Es la única manera de hacer su trabajo correctamente, de identificar vulnerabilidades y amenazas reales. Pero ese acceso debe estar estrictamente limitado al alcance del trabajo acordado y debe regirse por un principio de "necesidad de saber".

Para garantizar que no se abuse de ese acceso, se necesitan varias medidas:

- **Acuerdos de confidencialidad robustos:** Que establezcan las responsabilidades de la empresa de ciberseguridad y las consecuencias de cualquier violación.
- **Contratos claros y detallados:** Que especifiquen qué tipo de información se va a acceder, con qué fines y durante cuánto tiempo.
- **Controles de acceso estrictos:** Limitar el acceso a la información sensible solo a los empleados que realmente lo necesitan y registrar todas las acciones que realizan.
- **Supervisión independiente:** Auditorías externas o la presencia de representantes del cliente durante las partes más sensibles del proceso.
- **Transparencia:** Comunicación abierta y honesta con el cliente sobre el proceso de auditoría y los hallazgos.

¿Qué Mecanismos de Supervisión y Control Deberían Implementarse en las Empresas de Ciberseguridad Para Evitar que sus Empleados Utilicen Herramientas Avanzadas de Análisis Forense con Fines no Autorizados o Éticamente Cuestionables?

Prevenir el uso de herramientas avanzadas de análisis forense para fines no autorizados o éticamente cuestionables es crucial. Las siguientes son algunas medidas que se podrían implementar:

- **Auditorías internas aleatorias:** Para revisar los registros de uso de las herramientas de análisis forense y detectar cualquier anomalía.
- **Capacitación ética regular:** Para sensibilizar a los empleados sobre los riesgos y las consecuencias de las malas prácticas.
- **Políticas internas claras:** Que definan qué usos de las herramientas son aceptables y cuáles no.
- **Separación de funciones:** Limitar el acceso a las herramientas avanzadas de análisis forense solo a un grupo selecto de empleados, de acuerdo con su rol y con una supervisión más estricta.
- **Sistemas de registro y monitoreo:** Que registren todas las acciones realizadas con las herramientas de análisis forense, incluyendo quién las usó, cuándo y para qué.

¿Cómo Deberían Responder los Gobiernos y Organizaciones Cuando Descubren que una Empresa de Ciberseguridad Contratada ha Cometido Actos de Ciber espionaje? ¿Cuáles Serían las Medidas Adecuadas para Restaurar la Confianza y Asegurar que no Ocurra Nuevamente?

La respuesta de los gobiernos y organizaciones a un caso de ciber espionaje por parte de una empresa de ciberseguridad debe ser contundente y debe contemplar:

- **Acciones legales:** Persecución penal de los individuos involucrados y demandas civiles contra la empresa por daños y perjuicios.
- **Investigación exhaustiva:** Para determinar el alcance del daño y la identidad de los responsables.
- **Revisión de las regulaciones:** Para fortalecer los controles sobre las empresas de ciberseguridad y prevenir futuros incidentes.

Con el fin de restaurar la confianza por parte de los clientes y tratando de asegurar que no se vuelvan a presentar este tipo de casos se deben implementar las siguientes medidas:

- **Sanciones severas:** Multas elevadas, revocación de licencias o incluso la prohibición de operar en el sector público.

Para restaurar la confianza debe:

- **Compensación a las víctimas:** Ofrecer reparaciones por los daños sufridos.
- **Fomento de la colaboración:** Entre gobiernos, empresas y la sociedad civil para combatir el ciber espionaje y otras amenazas cibernéticas.
- **Reformas en la industria:** Promover la adopción de mejores prácticas éticas y estándares de conducta más estrictos.
- **Transparencia total:** Divulgar los detalles del incidente al público y a los clientes afectados.

Describir de Manera Específica las Herramientas Software que Utilizó Para Llevar a Cabo el Anexo 4 – Escenario 3 Enfocado A RedTeam

Evidencia de los Comandos Utilizados y Resultados que Arrojó Cada Herramienta Utilizada, Estas Herramientas Deben Estar Clasificadas Según los Pasos de un Pentesting

Planificación. Con la información suministrada en el Anexo 4 – Escenario 3 se define el alcance del pentesting, los sistemas a evaluar, los objetivos específicos y las reglas de compromiso.

Alcance. Se centra en la investigación de una posible fuga de información originada en un equipo específico dentro de la organización. El alcance principal será la evaluación de la seguridad de este equipo en particular y la aplicación vulnerable identificada.

Sistemas Por Evaluar. El sistema principal bajo la lupa es el equipo de cómputo señalado, que opera bajo Windows 7 y ejecuta una aplicación con una vulnerabilidad conocida. Adicionalmente, se investigará la posibilidad de escalación de privilegios dentro del sistema operativo.

Objetivos Específicos. El objetivo primordial es confirmar la existencia de la vulnerabilidad en la aplicación y determinar si esta puede ser explotada para acceder al sistema. De confirmarse la explotación, se buscará demostrar la capacidad de escalar privilegios mediante la creación de una cuenta de administrador, como prueba de concepto para la dirección.

Reglas de Compromiso. Para llevar a cabo esta evaluación, se utilizará una copia forense del servidor proporcionada. En caso de lograr un acceso privilegiado, se procederá a crear un usuario administrador con mi nombre y apellido como una demostración controlada del riesgo identificado.

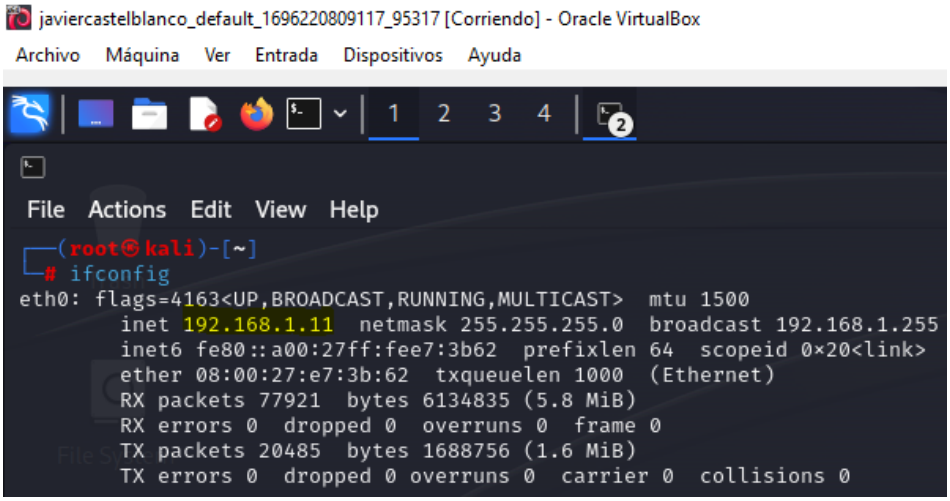
Reconocimiento. Se realiza la recopilación de información sobre la máquina objetivo con Windows 7 con el fin de entender su infraestructura de red, sistemas operativos, aplicaciones web, usuarios y posibles vulnerabilidades.

En este caso se utilizarán técnicas de recolección activa interactuando con la máquina objetivo Windows 7.

Para realizar la prueba de penetración se utilizará una máquina Kali Linux que tiene dirección IP 192.168.1.11.

Figura 16

Dirección IP de la máquina Kali Linux



Nota: *Información de la configuración de red de la máquina Kali Linux.*

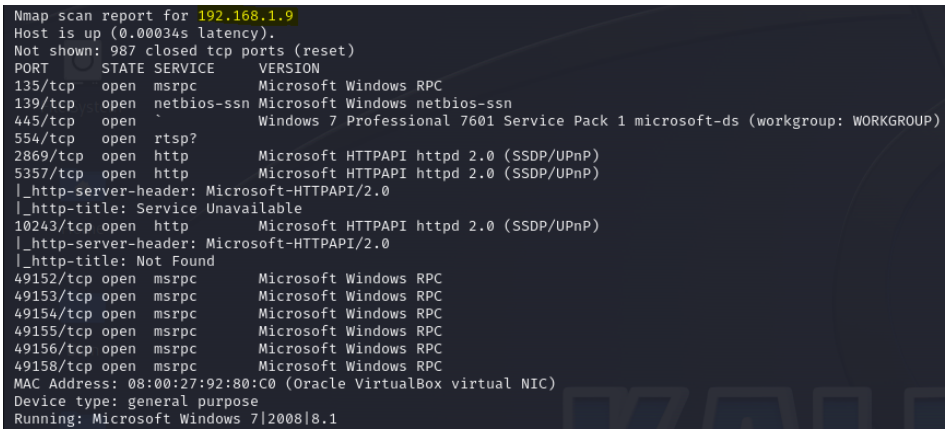
Se utiliza la **herramienta Nmap** (*Nmap: the Network Mapper - Free Security Scanner*, 2025) para realizar el reconocimiento de la máquina objetivo Windows 7.

Para localizar otros hosts en esta red LAN, se ejecuta el comando **nmap -A -T4 192.168.1.0/24**.

Como resultado del comando ejecutado se obtiene la dirección IP de la máquina objetivo con Windows 7 la cual es 192.168.1.9.

Figura 17

Dirección IP máquina objetivo Windows 7



Nota: *Información de la dirección IP la máquina objetivo con Windows 7.*

De igual manera se obtiene la información del estado de los puertos (en este caso los que están abiertos), los servicios disponibles y la versión.

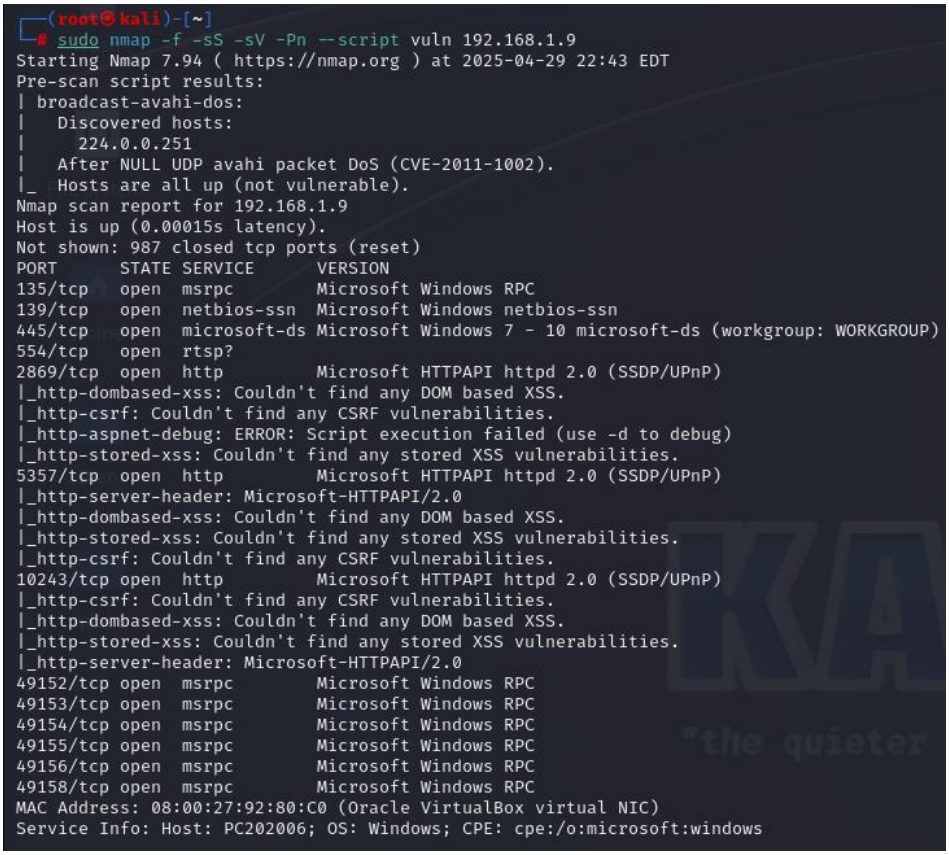
Se puede establecer que la máquina objetivo Windows 7 tiene sistema operativo Windows 7 Professional 7601 Service Pack 1.

Escaneo y Análisis. Se utiliza la **herramienta Nmap** para realizar el escaneo de vulnerabilidades en la máquina objetivo Windows 7 con el fin de identificar fallos de seguridad conocidos.

Se ejecuta el comando **sudo nmap -f -sS -sV -Pn --script vuln 192.168.1.9**

Figura 18

Escaneo de vulnerabilidades a la máquina objetivo Windows 7

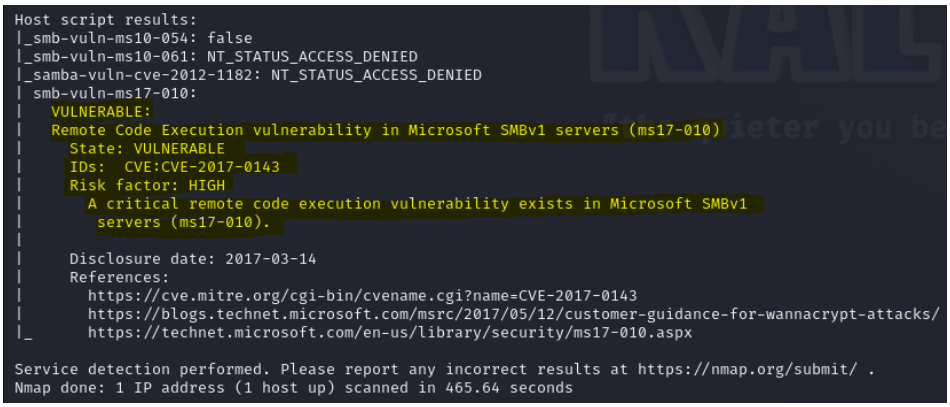


Nota: *Búsqueda de vulnerabilidades en la máquina objetivo Windows 7.*

Como resultado del comando se evidencian las vulnerabilidades encontradas.

Figura 19

Resultado de vulnerabilidades encontradas en la máquina objetivo Windows 7



Nota: *Vulnerabilidades encontradas en la máquina objetivo Windows 7.*

Una vez recopilada la información, se analizan las posibles vulnerabilidades presentes en la máquina objetivo Windows 7.

Se encontró que la máquina objetivo Windows 7 es vulnerable debido a que existe una vulnerabilidad crítica de ejecución remota de código en servidores Microsoft SMBv1 (ms17-010) la cual se encuentra detallada en la CVE-2017-0143 (*CVE -CVE-2017-0143*, 2017) y presenta un factor de riesgo alto.

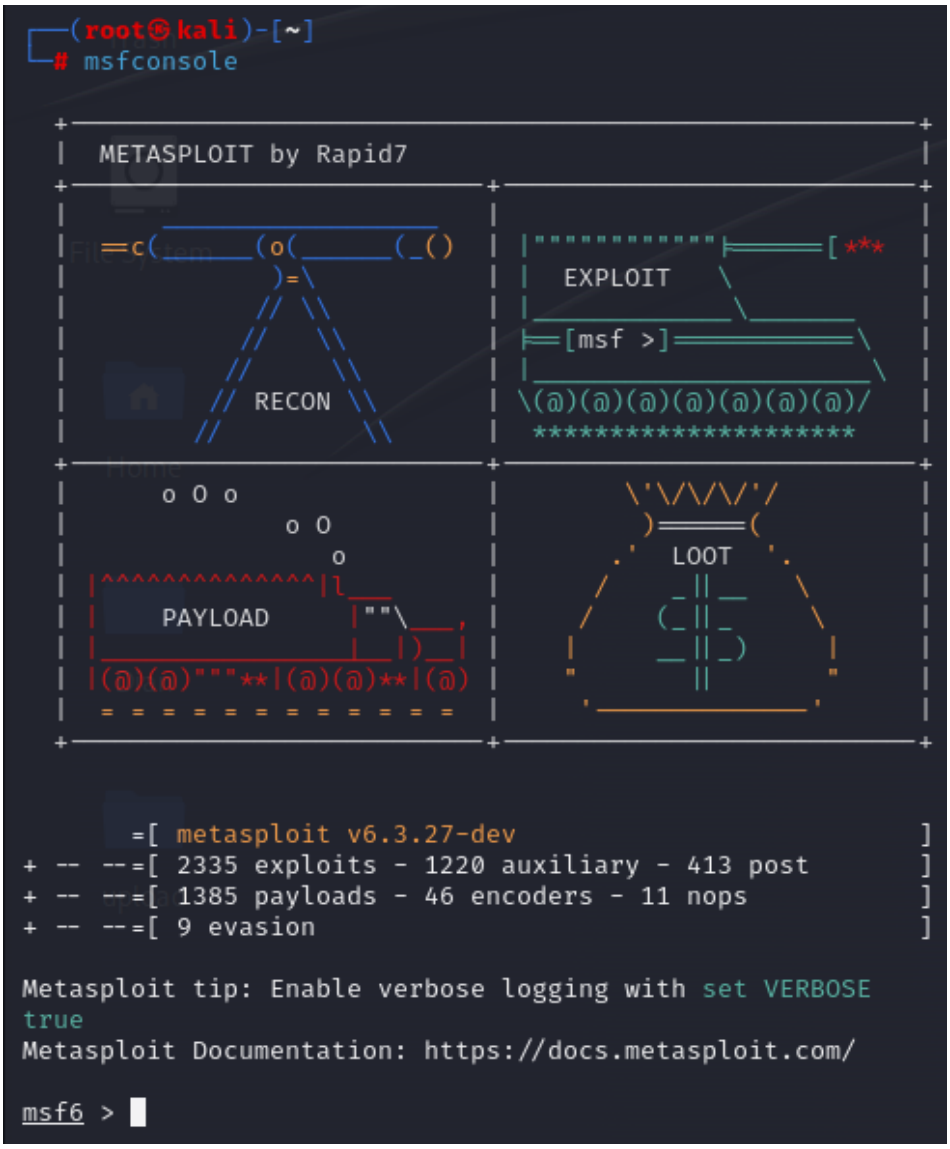
La vulnerabilidad encontrada se conoce también como EternalBlue, y es explotada por los ransomware Petya y WannaCry, entre otros. (*smb-vuln-ms17-010 NSE script — Nmap Scripting Engine documentation*, 2017)

Explotación. Se utiliza la **herramienta Metasploit Framework** con el fin de explotar la vulnerabilidad identificada para lograr el ingreso no autorizado a la máquina objetivo Windows 7.

En la máquina Kali Linux se inicia la consola de la **herramienta Metasploit Framework** mediante la utilización del comando **msfconsole**.

Figura 20

Inicio de la herramienta Metasploit Framework

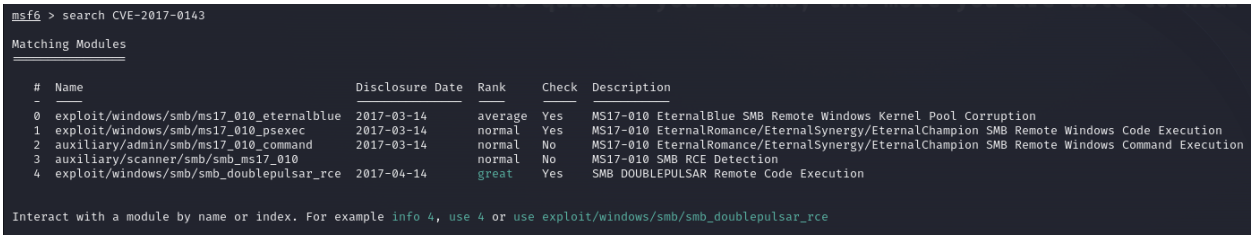


Nota: *Consola de la herramienta Metasploit Framework.*

En la consola de la **herramienta Metasploit Framework** se realiza la búsqueda de la vulnerabilidad CVE-2017-0143 mediante el comando **search CVE-2017-0143**

Figura 21

Búsqueda de la vulnerabilidad CVE-2017-0143

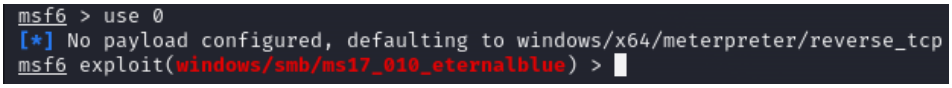


Nota: *Resultados de la búsqueda de la vulnerabilidad CVE-2017-0143 en la herramienta Metasploit Framework.*

El exploit MS17-010 EternalBlue se selecciona con la opción 0 exploit/windows/smb/ms17_010_eternalblue mediante el comando **use 0**.

Figura 22

Selección del módulo 0 exploit/windows/smb/ms17_010_eternalblue

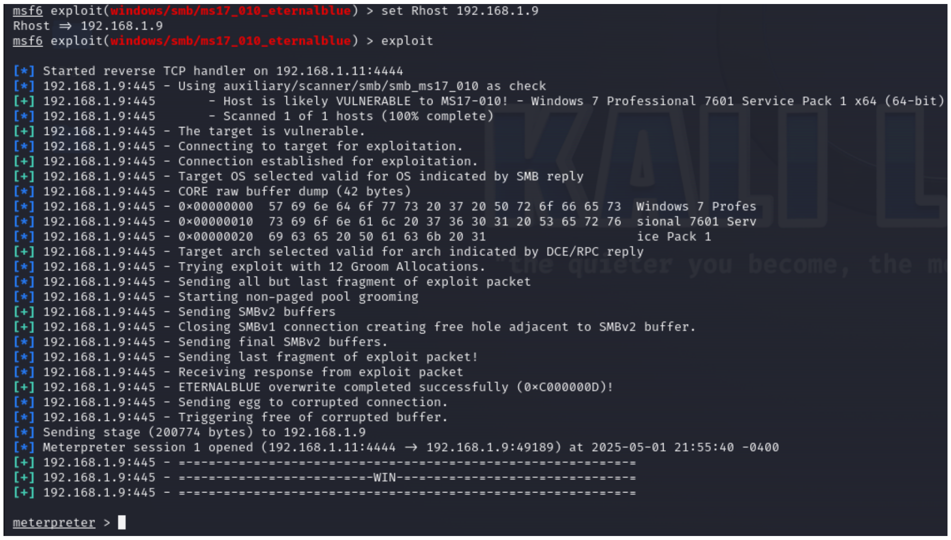


Nota: *Selección del exploit MS17-010 EternalBlue.*

Se configura la dirección IP de la máquina objetivo Windows 7 con el fin de explotarle la vulnerabilidad mediante el comando **set Rhost 192.168.1.9**, se inicia la explotación a través del puerto 445 mediante el comando **exploit** y como resultado se inicia el Meterpreter (carga útil o payload).

Figura 23

Configuración de la IP de la máquina objetivo e inicio de la explotación



Nota: *Configuración de la dirección IP de la máquina objetivo Windows 7 y ejecución del exploit.*

Una vez se inicia el Shell de Meterpreter se puede pasar a la fase de post-explotación.

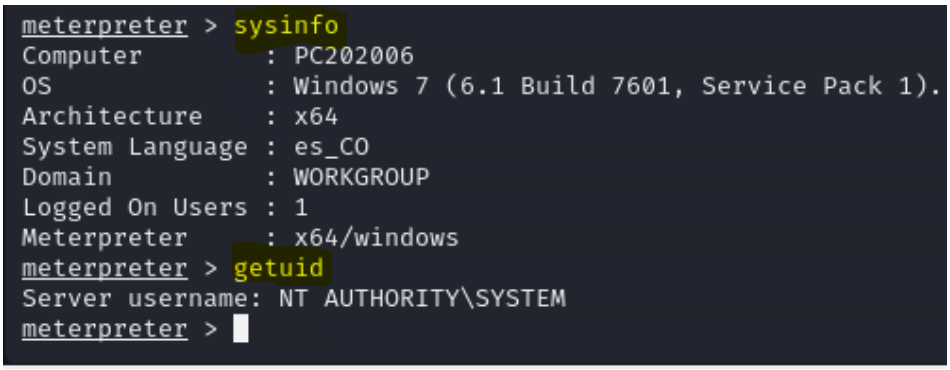
Post-explotación y Mantenimiento del Acceso. Después de obtener acceso a la máquina objetivo Windows 7, se evalúa el impacto del ataque y la capacidad del atacante para mantener el acceso al sistema.

Se busca información detallada de la configuración de la máquina objetivo Windows 7 mediante el comando **sysinfo**, obteniendo como resultado el nombre del host, el sistema operativo, la arquitectura, el lenguaje del sistema, el nombre del dominio, los usuarios registrados.

Con el comando **getuid** se busca información del usuario conectado, la cual se puede utilizar para elevar privilegios y se exploran las posibilidades de movimientos laterales dentro de la red.

Figura 24

Información de la configuración de la máquina objetivo Windows 7



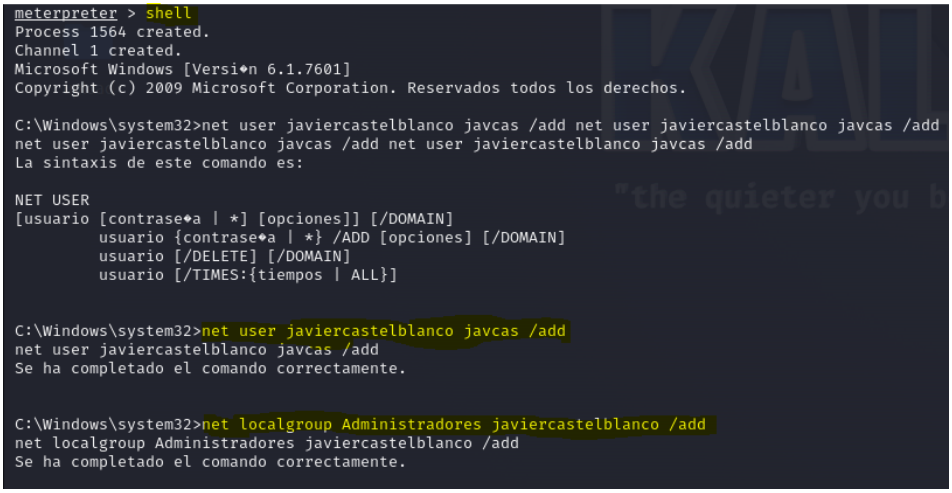
Nota: *Nombre del host, sistema operativo, arquitectura, lenguaje del sistema, nombre del dominio, usuarios registrados.*

Como resultado se obtiene que la cuenta del usuario conectado es NT AUTHORITY\SYSTEM o conocida simplemente como SYSTEM, la cual tiene los privilegios más altos en el sistema de la máquina objetivo Windows 7, por lo cual no se hace necesario escalar privilegios.

Mediante el comando **shell** se ingresa a la línea de comando de la máquina objetivo Windows 7, se procede a crear el usuario javiercastelblanco con contraseña javcas utilizando el comando **net user javiercastelblanco javcas /add** y se le asignan permisos de administrador mediante el comando **net localgroup Administradores javiercastelblanco /add**

Figura 25

Creación de usuario con permisos de administrador en la máquina objetivo Windows 7



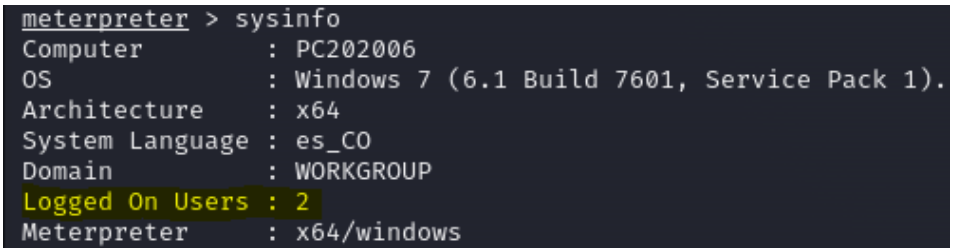
Nota: *Creación del usuario javiercastelblanco y asignación de permisos de administrador en la máquina objetivo Windows 7.*

Con la creación del usuario javiercastelblanco y la asignación de permisos de administración se mantiene el acceso en la máquina objetivo Windows 7.

En el meterpreter se ejecuta el comando **sysinfo** y se puede evidenciar que después de la creación del usuario javiercastelblanco aparecen dos (2) usuarios registrados en la máquina objetivo Windows 7.

Figura 26

Usuarios registrado en la máquina objetivo Windows 7



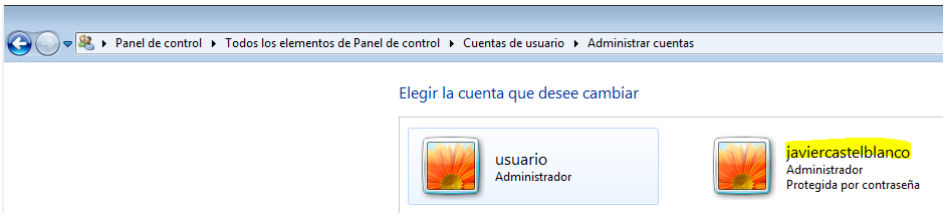
Nota: *Dos (2) usuarios registrados en la máquina objetivo después de la creación del usuario javiercastelblanco.*

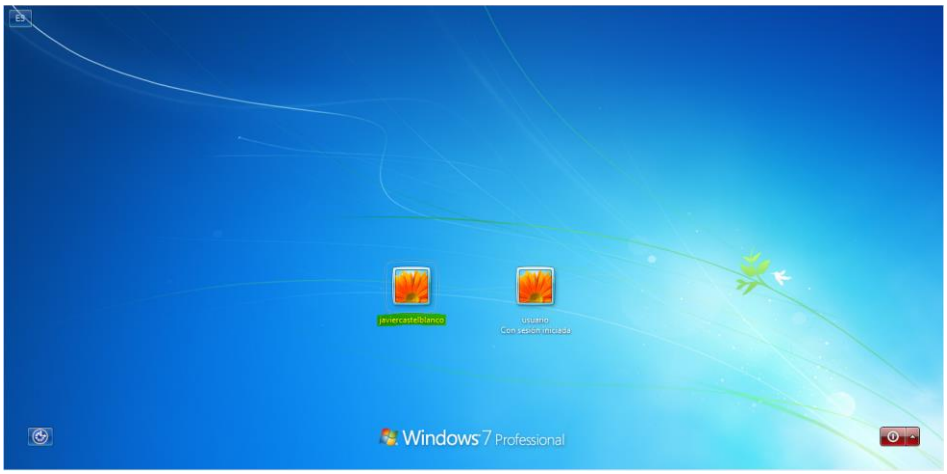
En la máquina objetivo Windows 7 se puede evidenciar que el usuario javiercastelblanco fue creado y que cuenta con privilegios de administrador demostrando de esa manera que la máquina objetivo Windows 7 fue vulnerada, se explotó la vulnerabilidad CVE-2017-0143.

Debido a que el usuario javiercastelblanco creado en la máquina objetivo Windows 7 cuenta con permisos de administrador, permite al atacante persistencia en el acceso al sistema en caso de que se cierre la vulnerabilidad explotada, manteniendo así un acceso prolongado en el sistema de la máquina objetivo Windows 7.

Figura 27

Evidencia de la creación del usuario administrador en la máquina objetivo Windows 7





Nota: *Usuario javiercastelblanco con privilegios de administrador.*

Análisis y Reporte. Se documentan de forma detallada todos los resultados y los hallazgos del pentesting, presentando un informe detallado para los responsables de la organización objetivo.

El informe de la prueba de penetración realizada describe el impacto potencial de la vulnerabilidad detectada, el exploit utilizado, las pruebas realizadas y recomendaciones para mitigarla y mejorar la seguridad. Este informe se puede visualizar en la página 25 de este trabajo.

Liste y Describa los Datos e Información del Anexo 4 – Escenario 3 que le Fueron de Ayuda Para Identificar el Fallo de Seguridad Específico el Cual Ataca a la Máquina Windows

Informe con Análisis del Caso de Red Team, que Permitió dar Solución al Fallo Identificado

Naturaleza del Problema: "fuga de información... al interior de la organización en uno de sus equipos de cómputo en la dependencia."

El problema es una exfiltración de datos originada internamente, localizada en un equipo específico dentro de un área o departamento.

Esto define el objetivo principal que es detener la fuga de información y delimita el perímetro inicial de investigación a un equipo específico dentro de la red interna. Inicialmente se tiene conocimiento que no se está buscando una brecha perimetral, sino un compromiso interno ya existente o una vulnerabilidad que está siendo explotada desde dentro o que permite acceso persistente. La mención de "dependencia" puede dar pistas sobre el tipo de información en riesgo y los posibles actores o niveles de acceso involucrados.

Sistema Operativo del Objetivo: "máquina... bajo un windows."

El sistema operativo del equipo afectado es Windows, este es un dato fundamental ya que orienta toda la estrategia de la prueba de penetración debido a que las herramientas a utilizar deben ser compatibles con Windows, los tipos de vulnerabilidades son comunes a servicios de Windows, al Active Directory, y a software comúnmente instalado en Windows, las técnicas de post-explotación mediante el uso de exploits de kernel específicos de Windows, y metodologías de evasión de una herramienta EDR o de Antivirus predominantes en Windows.

Vector de Ataque Principal: "tiene instalada una aplicación vulnerable."

Se sospecha que la causa raíz o el punto de entrada es una aplicación específica instalada en la máquina Windows, esto centra la fase de reconocimiento y enumeración. El equipo

RedTeam debe identificar todas las aplicaciones instaladas en esa máquina y priorizar la investigación sobre aquellas conocidas por tener vulnerabilidades, especialmente las que manejan datos sensibles o interactúan con la red. Se define una superficie de ataque clara: la aplicación y sus componentes.

Existencia de un Exploit Potencialmente Conocido: "esta aplicación al parecer tiene asociado un exploit."

Existe información preliminar de inteligencia que sugiere que hay un exploit disponible o conocido para la aplicación vulnerable identificada, lo que incrementa significativamente la probabilidad de compromiso activo. Impulsa la búsqueda activa de CVEs (Common Vulnerabilities and Exposures) asociadas a las aplicaciones candidatas y la búsqueda de PoCs (Proofs of Concept) o exploits funcionales en bases de datos públicas y privadas. Esta información le permite al Red Team intentar replicar el ataque para confirmar la vulnerabilidad y entender el mecanismo exacto de la brecha.

Impacto Potencial del Exploit: "puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque."

El exploit asociado a la aplicación podría permitir ejecución remota de comandos, obtención de permisos elevados u otras acciones maliciosas. Describe los posibles resultados directos de explotar la vulnerabilidad. El acceso Shell es crítico para la toma de control remoto. La escalación de privilegios es clave para moverse lateralmente, acceder a más datos y establecer persistencia robusta. La frase "Otro tipo de ataque" es incierta, pero mantiene abierta la posibilidad a otros impactos como denegación de servicio, manipulación de datos, etc., aunque el foco principal parece ser el control y la exfiltración.

Línea de Investigación Específica: "también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema."

Se considera activamente una técnica específica de escalada de privilegios: la creación de una nueva cuenta con derechos de administrador, proporcionando una hipótesis concreta y verificable. Con esta información el equipo RedTeam puede buscar activamente en los logs de eventos de seguridad la creación de usuarios recientes, o intentar explotar la vulnerabilidad inicial con el objetivo específico de crear dicho usuario. También sugiere un posible indicador de compromiso (IOC) a buscar: cuentas de administrador desconocidas o sospechosas en el sistema.

El Anexo 4 – Escenario 3 proporciona información crucial que permite al Red Team pasar de un problema general de fuga de información a un plan de acción técnico y enfocado: localizar una máquina Windows específica, identificar aplicaciones instaladas, investigar vulnerabilidades conocidas (particularmente una con un exploit asociado que permita shell o escalada), y verificar una técnica de escalada específica (creación de usuario administrador). Cada pieza de información refina la búsqueda y guía la selección de herramientas y técnicas para validar la hipótesis y reproducir el ataque que causa la fuga de datos.

¿Qué Herramienta Utilizó Para Poder Identificar los Fallos de Seguridad de la "Máquina Windows"? ¿Qué Puerto Abre la Aplicación Específica en el Anexo?

Informe de Herramientas Utilizadas Para Identificar Fallos en el Escenario Propuesto

Se utilizó la **herramienta Nmap** para realizar el escaneo de vulnerabilidades en la máquina objetivo Windows 7 con el fin de identificar fallos de seguridad conocidos.

Se ejecutó el comando **sudo nmap -f -sS -sV -Pn --script vuln 192.168.1.9** para realizar un escaneo exhaustivo sobre la máquina objetivo Windows 7 con dirección IP 192.168.1.9 buscando identificar posibles vulnerabilidades.

El comando realiza las siguientes acciones sobre la máquina objetivo Windows 7 con dirección IP 192.168.1.9:

-f -sS: Envía paquetes SYN fragmentados para intentar evadir la detección y realizar un escaneo de puertos TCP de manera sigilosa.

-sV: Intenta determinar la versión de los servicios que se encuentran escuchando en los puertos abiertos.

-Pn: Asume que el host está activo.

--script vuln: Ejecuta scripts de la categoría "vuln" para identificar automáticamente posibles vulnerabilidades en los servicios detectados.

El puerto que abre la aplicación vulnerable es el 445, el cual para Microsoft está asociado al protocolo SMB (Server Message Block), en sistemas Windows puede tener vulnerabilidades que permiten a los atacantes ejecutar código de forma remota.

Explique Con Sus Palabras y de Manera Específica Cómo Afecta el Ataque a la Máquina (Windows), Haga Uso de Gráficos Para Explicar el Ataque.

Análisis del Ataque Presentado a Cada una de las Máquinas Identificadas

Fase 1: Recolección de Información y Descubrimiento. En esta etapa inicial, el objetivo es identificar sistemas activos en la red y los servicios que están ejecutando. Usando herramientas de escaneo de puertos, como Nmap, se puede descubrir que el puerto 445 (asociado al servicio SMB) está abierto en la dirección IP de la máquina Windows 7.

Fase 2: Análisis de Vulnerabilidades. Una vez se identifica que el servicio SMB está corriendo, la siguiente etapa es investigar si existen vulnerabilidades conocidas asociadas a él en un sistema Windows 7. A través de una base de datos de vulnerabilidades, se puede identificar la vulnerabilidad CVE-2017-0143, la cual es la que explota "eternalblue".

Fase 3: Explotación. En esta fase es donde se utiliza el exploit "eternalblue". Este exploit se dirige específicamente a la forma en que el servicio SMB de Windows 7 maneja ciertos tipos de peticiones.

El servicio SMB es el encargado de gestionar el acceso a archivos compartidos en la red. La vulnerabilidad CVE-2017-0143 reside en una parte específica de este servicio que maneja los "paquetes" de comunicación. "Eternalblue" envía un paquete especialmente diseñado que aprovecha un error en esta forma de manejo.

Al recibir este paquete malicioso, el servicio SMB no lo procesa correctamente. En lugar de eso, ocurre un desbordamiento de memoria. De esta manera, el paquete de "eternalblue" sobrepasa la capacidad de una parte de la memoria del servicio SMB.

Este desbordamiento de memoria permite al atacante sobrescribir ciertas partes importantes de la memoria del sistema operativo donde se está ejecutando el servicio SMB. Al

sobrescribir estas áreas críticas con código malicioso propio (payload), se engaña al sistema para que ejecute ese código en lugar de lo que normalmente haría.

Fase 4: Post-Explotación. Una vez que el código malicioso (payload) se ejecuta en el sistema Windows 7, las posibilidades son amplias. Normalmente, este payload proporciona algún tipo de acceso al sistema. Esto podría ser una "shell" remota, que es como tener una línea de comandos directamente en la máquina comprometida.

Con este acceso, se pueden realizar diversas acciones, dependiendo de los objetivos en la prueba de penetración. Esto podría incluir:

- Explorar el sistema de archivos: Buscar información sensible.
- Escalar privilegios: Intentar obtener derechos de administrador si nuestro acceso inicial es limitado.
- Movimiento lateral: Intentar comprometer otros sistemas dentro de la misma red utilizando la máquina comprometida como punto de apoyo.
- Instalar puertas traseras (backdoors): Para mantener el acceso al sistema en el futuro.

Es fundamental entender que "eternalblue" es una herramienta poderosa porque permite la ejecución remota de código sin necesidad de interacción por parte del usuario. Simplemente enviando el paquete malicioso a un sistema vulnerable, se puede lograr el compromiso. Esta es la razón por la que fue tan devastador en ataques como WannaCry.

Documente Cada uno de los Pasos que Ejecutó y sus Respectivas Evidencias Para Explotar la Vulnerabilidad en la Máquina Windows 7.

Informe de la Explotación de Vulnerabilidades en el Escenario Propuesto Evidencia de la Explotación de la Vulnerabilidad Identificada

INFORME CONFIDENCIAL DE PRUEBA DE PENETRACIÓN

Objetivo del Informe: Evaluar la seguridad de la máquina objetivo Windows 7 con dirección IP 192.168.1.9 y determinar el impacto potencial de las vulnerabilidades explotables identificadas durante el ejercicio de Red Team.

1. Resumen Ejecutivo

Durante la prueba de penetración dirigida a la máquina objetivo Windows 7 con dirección IP 192.168.1.9, se identificó una vulnerabilidad crítica CVE-2017-0143, asociada al servicio SMBv1. Se confirmó la explotabilidad de esta vulnerabilidad utilizando el exploit conocido como MS17-010 "EternalBlue" a través del Metasploit Framework. La explotación de la vulnerabilidad fue exitosa ya que se obtuvo el **acceso no autorizado con privilegios de nivel SYSTEM** a la máquina objetivo Windows 7. Como prueba de control y para demostrar el impacto, se procedió a crear una cuenta de usuario local (javiercastelblanco) con contraseña (javcas) y se le asignaron privilegios de administrador. Este hallazgo representa un **riesgo crítico** para la confidencialidad, disponibilidad e integridad del sistema afectado y potencialmente para la red interna, ya que permite a un atacante tomar control total del equipo, exfiltrar datos, instalar malware persistente o utilizarlo como pivote para ataques posteriores (movimiento lateral). Se requiere una **acción correctiva inmediata**.

2. Alcance y Metodología

- **Alcance:** La prueba de penetración se enfocó específicamente en el sistema operativo Microsoft Windows 7 y los servicios expuestos por la máquina objetivo Windows 7 con dirección IP 192.168.1.9.
- **Metodología:** Se siguió una metodología estándar de pruebas de penetración:
    - **Reconocimiento:** Escaneo de puertos y servicios utilizando Nmap para identificar servicios activos y posibles vectores de ataque. **(Páginas 8 y 9 de este trabajo).**
    - **Análisis de Vulnerabilidades:** Correlación de los servicios y versiones identificados con bases de datos de vulnerabilidades conocidas (CVE). Se detectó el puerto 445/tcp abierto y vulnerable a MS17-010 (CVE-2017-0143) mediante scripts de Nmap (smb-vuln-ms17-010.nse). **(Páginas 10 y 11 de este trabajo).**
    - **Explotación:** Intento controlado de explotación de la vulnerabilidad CVE-2017-0143 utilizando el módulo exploit/windows/smb/ms17_010_eternalblue dentro del Metasploit Framework. **(Páginas 12, 13 y 14 de este trabajo).**
    - **Post-Explotación:** Una vez obtenido el acceso (sesión Meterpreter con privilegios SYSTEM), se realizaron acciones para demostrar el nivel de control alcanzado, incluyendo la creación de un usuario administrador persistente. **(Páginas 15, 16 y 17 de este trabajo).**

3. Hallazgo Detallado: CVE-2017-0143 - Ejecución Remota de Código vía SMBv1 (MS17-010 EternalBlue)

- **Descripción:** El servicio Server Message Block versión 1 (SMBv1) en la máquina objetivo Windows 7 (192.168.1.9) presenta una vulnerabilidad crítica (CVE-2017-0143) que permite la ejecución remota de código arbitrario sin autenticación. Esta

vulnerabilidad es explotada por el conocido exploit "EternalBlue", parte del set de herramientas MS17-010.

- **Evidencia:**
    - Nmap identificó el puerto 445/tcp (SMB) como abierto. **(Página 10 de este trabajo).**
    - El script smb-vuln-ms17-010.nse de Nmap marcó el host como VULNERABLE. **(Página 11 de este trabajo).**
    - Se utilizó Metasploit (msfconsole) configurando el exploit exploit/windows/smb/ms17_010_eternalblue con RHOST=192.168.1.9. **(Páginas 13 y 14 de este trabajo).**
    - La ejecución del exploit resultó en una sesión de Meterpreter con privilegios NT AUTHORITY\SYSTEM. **(Página 15 de este trabajo).**
- **Severidad: CRÍTICA**

4. Impacto Potencial Detallado

La explotación exitosa de CVE-2017-0143 en la máquina objetivo Windows 7 con dirección IP 192.168.1.9 de forma inmediata tiene consecuencias con severidad alta:

- **Compromiso Total del Sistema:** Un atacante obtiene control absoluto (privilegios SYSTEM) sobre la máquina objetivo Windows 7.
- **Denegación de Servicio (DoS):** Un atacante podría corromper el sistema operativo, borrar archivos críticos o cifrar el disco duro, dejando el equipo inutilizable.
- **Escalada de Privilegios en Dominio:** Si el equipo está unido a un dominio y se obtienen credenciales de dominio, el riesgo se extiende a toda la infraestructura de Active Directory.

- **Exfiltración de Datos:** Acceso total a todos los archivos almacenados localmente, incluyendo documentos sensibles, credenciales cacheadas, correos electrónicos, etc.
- **Instalación de Malware Persistente:** Capacidad para instalar cualquier tipo de software malicioso (backdoors, ransomware, spyware, troyanos) que puede sobrevivir reinicios y evadir detecciones básicas.
- **Pérdida de Reputación y Confianza:** Si el compromiso resulta en una brecha de datos pública.
- **Pivote para Movimiento Lateral:** El equipo comprometido puede ser utilizado como punto de referencia para lanzar ataques a otros sistemas dentro de la misma red, escalando el compromiso.

5. Pruebas Realizadas y Acciones Post-Explotación

Tras obtener la sesión de Meterpreter con privilegios SYSTEM en la máquina objetivo Windows 7 (192.168.1.9), se ejecutaron los siguientes comandos para demostrar el control y establecer una forma de persistencia básica:

1. meterpreter > sysinfo (Información sobre la máquina objetivo Windows 7, nombre, tipo de sistema operativo, arquitectura, dominio e idioma).
2. meterpreter > shell (Acceso a línea de comando cmd.exe en la máquina objetivo Windows 7).
3. C:\Windows\system32> net user javiercastelblanco javcas /add (Creación del usuario local 'javiercastelblanco' con contraseña 'javcas').
4. C:\Windows\system32> net localgroup Administradores javiercastelblanco /add (Adición del nuevo usuario al grupo local de Administradores).

Estas acciones confirman que un atacante puede crear cuentas privilegiadas para mantener el acceso al sistema comprometido, incluso si la vulnerabilidad original es parcheada posteriormente (siempre que la cuenta no sea eliminada).

6. Recomendaciones de Mitigación y Fortalecimiento

Es **necesario** abordar esta vulnerabilidad de forma inmediata:

- **Remediación Inmediata (Urgente):**
    1. **Aplicar el Parche MS17-010:** Instalar la actualización de seguridad oficial de Microsoft MS17-010 que corrige la vulnerabilidad CVE-2017-0143. Esta es la medida más crítica y efectiva.
    2. **Deshabilitar SMBv1:** Si la funcionalidad de SMBv1 no es estrictamente necesaria para operaciones críticas, se debe deshabilitar siguiendo las guías de Microsoft. Esto elimina el vector de ataque principal para EternalBlue. Se puede hacer vía PowerShell o modificando el registro.
    3. **Eliminar Usuario Creado:** Eliminar la cuenta de usuario javiercastelblanco creada durante la prueba de penetración.
- **Recomendaciones a Corto Plazo:**
    1. **Actualizar/Migrar Windows 7:** El sistema operativo Windows 7 ha llegado al final de su vida útil y ya no recibe actualizaciones de seguridad de Microsoft. **Es fundamental planificar y ejecutar la migración de este equipo a una versión de Windows soportada (Windows 10, Windows 11) o a otro sistema operativo con soporte activo.** Mantener Windows 7 representa un riesgo de seguridad inaceptable a largo plazo.

2. **Segmentación de Red:** Aislar los sistemas que no puedan ser parcheados o actualizados inmediatamente en segmentos de red restringidos para limitar el impacto de un compromiso.
3. **Firewall de Host y Perimetral:** Configurar firewalls para bloquear el tráfico SMB (puerto TCP 445) entrante desde redes no confiables y, si es posible, restringir la comunicación SMB incluso dentro de la red local solo a los hosts que legítimamente la necesiten.

- **Recomendaciones Estratégicas (Largo Plazo):**
  1. **Auditorías de Seguridad Periódicas:** Llevar a cabo pruebas de penetración y auditorías de seguridad internas y externas periódicamente con el fin de detectar y mitigar vulnerabilidades antes de que sean explotadas por atacantes reales.
  2. **Gestión de Vulnerabilidades y Parchado:** Implementar un programa robusto para escanear regularmente la red en busca de vulnerabilidades y asegurar la aplicación oportuna de parches de seguridad en todos los sistemas.
  3. **Monitorización de Seguridad:** Desplegar y mantener sistemas de detección de intrusos (IDS/IPS) y un SIEM (Security Information and Event Management) para detectar actividad sospechosa, como escaneos de SMB o intentos de explotación.
  4. **Principio de Menor Privilegio:** Asegurar que los usuarios y servicios operen con los mínimos privilegios necesarios para realizar sus funciones.

7. Conclusión

La prueba de penetración ha demostrado exitosamente que la máquina objetivo Windows 7 con dirección IP 192.168.1.9 es vulnerable a ejecución remota de código a través de CVE-

2017-0143 (EternalBlue). Se obtuvo control total del sistema (privilegios SYSTEM) y se creó un usuario administrador local como prueba de concepto - PoC. Este hallazgo representa un riesgo crítico que requiere atención inmediata. La aplicación del parche MS17-010 y la desactivación de SMBv1 son pasos urgentes. Sin embargo, la recomendación estratégica más importante es la **migración del sistema operativo Windows 7 a una versión con soporte activo** para mitigar riesgos futuros asociados a sistemas obsoletos.

Analizar un Caso de Ataque Informático en Tiempo Real e Identificar Las Acciones Que Debe Desarrollar Para Detectarlo y Contenerlo de Manera Exitosa

¿Qué Sería lo Primero Que Indagaría y Haría si Llegara a Encontrarse un Ataque en Tiempo Real? Especifique su Respuesta Con Argumentos Técnicos

Teniendo en cuenta el caso del Anexo 5 – Escenario 4, lo primero que haría en un escenario de un ataque en tiempo real en el cual se explota la vulnerabilidad CVE-2017-0143 (*CVE -CVE-2017-0143*, 2017) a una máquina con Windows 7, sería **tomar acciones urgentes para contener el daño evitando que el incidente de seguridad se agrave** y luego averiguar exactamente qué está sucediendo.

Pasos Iniciales de Respuesta e Investigación. Teniendo en cuenta que se está enfrentando un incidente en tiempo real y se necesita usar herramientas de código abierto:

- **Aislar el Sistema:**
    - **Acción:** Lo primero es desconectar la máquina Windows 7 comprometida de la red. Esto podría significar desenchufar físicamente el cable de red o deshabilitar el adaptador de red a través del sistema operativo si todavía se tiene acceso a la consola. Si es una máquina virtual, aislar su interfaz de red virtual.
    - **Argumento:** Esto es crucial para evitar que el atacante se mueva lateralmente dentro de la red, exfiltre más datos o use la máquina Windows 7 comprometida para atacar otros sistemas. Contener la amenaza es primordial. Dado que CVE-2017-0143 está relacionado con SMB explotado por WannaCry y NotPetya (*smb-vuln-ms17-010 NSE script* —

Nmap Scripting Engine documentation, 2017), que tiene capacidades de gusano, el aislamiento es aún más crítico para prevenir su propagación.

2. **Adquisición de Datos en Vivo (La Volatilidad es Clave):**
    - **Acción:** Antes de hacer cualquier cosa que pueda alterar significativamente el estado del sistema (como un reinicio, que se debe evitar inicialmente), se necesita capturar datos volátiles. Estos son datos que se perderán si la máquina se apaga.
    - **Herramientas y Argumentos:**
        - **Listado de Procesos:** Usar una herramienta como **Process Explorer** (*procexp.exe*, 2024) de Sysinternals que, aunque no es Licencia Pública General (GPL), es gratuita y ampliamente aceptada; para una alternativa estrictamente GPL, se puede buscar scripts usando Get-Process de PowerShell o la salida de tasklist.exe redirigida a un archivo. Se buscan procesos sospechosos, uso inusual de CPU/memoria o procesos ejecutándose desde ubicaciones extrañas.
        - **Conexiones de Red:** Ejecutar el comando **netstat -anob** (incorporado de Windows) o **TCPView** (*tcpview.exe*, 2023) de Sysinternals; o Get-NetTCPConnection en PowerShell para un enfoque programable es esencial. Se necesita ver todas las conexiones de red activas, los puertos de escucha y los PID de los procesos que las poseen. Buscar conexiones a IP maliciosas conocidas, puertos inusuales o conexiones realizadas por procesos

inesperados. Dado que CVE-2017-0143 explota SMB (puerto TCP 445), se debe prestar mucha atención a la actividad en este puerto.

- **Archivos Abiertos y Controladores (Handles):** Herramientas como **Handle** (*handle.exe*, 2022) de Sysinternals pueden mostrar qué archivos están siendo accedidos por qué procesos. Esto puede ayudar a identificar cargas útiles de malware, archivos de configuración que se están leyendo o datos que se están preparando para la exfiltración.
- **Volcado de Memoria (Condicional):** Si se tienen las herramientas y la experiencia disponibles de inmediato, y si la situación justifica una inmersión profunda por ejemplo, se sospecha de malware sin archivos, se debe considerar la captura de un volcado de memoria completo usando una herramienta GPL como **WinPmem** (Rasool, 2024). Este volcado puede analizarse posteriormente con herramientas GPL como Volatility Framework (*The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community*, 2025) para descubrir una gran cantidad de información, incluidos procesos en ejecución, artefactos de red, código inyectado y claves criptográficas. Sin embargo, esto lleva tiempo y podría posponerse si la contención inmediata es más crítica.
- **Archivos/Claves de Registro Modificados Recientemente:** Revisar los registros de eventos (Seguridad, Sistema, Aplicación)

usando el Visor de Eventos (eventvwr.msc) y buscar modificaciones recientes de archivos en ubicaciones comunes de persistencia de malware (por ejemplo, carpetas C:\ProgramData, AppData, Temp) y entradas sospechosas de ejecución automática en el registro (HKLM\Software\Microsoft\Windows\CurrentVersion\Run, HKCU\Software\Microsoft\Windows\CurrentVersion\Run).

3. **Identificar y Comprender el Vector de Ataque:**
    - **Acción:** Mientras se recopilan datos en vivo, se está formulando la hipótesis. Dada la vulnerabilidad conocida CVE-2017-0143, la principal sospecha sería un ataque basado en SMB.
    - **Argumento:** Se realiza la búsqueda de registros relacionados con el tráfico SMB (aunque el registro SMB nativo de Windows 7 podría ser limitado sin configuración previa). También se debe verificar la presencia de indicadores conocidos asociados con exploits para esta vulnerabilidad, como *named pipes* específicos o servicios creados por malware como WannaCry. Los registros del sistema podrían mostrar intentos fallidos de inicio de sesión o eventos de creación de servicios.
4. **Contención y Mitigación Inicial (Post-Aislamiento):**
    - **Acción:** Con base en los hallazgos de los pasos 2 y 3:
        - **Bloquear IPs/Dominios Maliciosos:** Si se identifican servidores C2 maliciosos, se deben bloquear en el firewall perimetral o en el

firewall basado en host (wf.msc) en otros sistemas si el parcheo inmediato no es posible.

- **Terminar Procesos Maliciosos:** Terminar cuidadosamente los procesos maliciosos identificados. Anotar la ruta del proceso y cualquier DLL asociada.
- **Deshabilitar Servicios/Tareas Comprometidas:** Si el malware ha establecido persistencia a través de un servicio o tarea programada, se debe deshabilitar.
- **Aplicación de Parches (si no se ha hecho ya):** Aunque esta máquina Windows 7 ya está comprometida, asegurar que MS17-010 (*smb-vuln-ms17-010 NSE script — Nmap Scripting Engine documentation*, 2017) el parche para CVE-2017-0143 se aplique *después* de neutralizar la amenaza inmediata y limpiar (o reconstruir) la máquina Windows 7 es vital para prevenir una reinfección. Para otras máquinas en la red, la aplicación inmediata de parches o la desactivación de SMBv1 sería una alta prioridad.

- **Argumento:** El objetivo aquí es detener la actividad maliciosa en el host Windows 7 y recopilar suficiente información para comprender el alcance y prevenir daños mayores.

Durante todo este proceso, una **documentación** detallada es la clave: marcas de tiempo, comandos ejecutados, observaciones y cualquier archivo recopilado. Esta información es crítica para el análisis profundo posterior, la recuperación y el informe post-incidente. El enfoque se

centra en acciones rápidas y metódicas para obtener control y visibilidad utilizando herramientas fácilmente disponibles y autorizadas.

Identificar y Proponer Medidas de Hardenización Adecuadas en un Escenario Real Para Evitar Ataques de Seguridad Informática

Teniendo en Cuenta el Ataque Ejecutado Desde el Ejercicio de Red Team, ¿Qué Medidas de Hardenización Propondría Para Que el Ataque no se Repita?

Medidas de Mitigación y Hardenización (Fortalecimiento). Por parte del equipo Blue Team se identificaron y propusieron las siguientes medidas de hardenización que pueden implementarse en el escenario propuesto, para evitar ataques de seguridad informática como el presentado en la máquina Windows 7 se repita, se hace **necesario** abordar la vulnerabilidad CVE-2017-0143 de forma inmediata:

- **Remediación Inmediata (Urgente):**
    1. **Aplicar el Parche MS17-010:** Instalar la actualización de seguridad oficial de Microsoft MS17-010 que corrige la vulnerabilidad CVE-2017-0143. Esta es la medida más crítica y efectiva.
    2. **Deshabilitar SMBv1:** Si la funcionalidad de SMBv1 no es estrictamente necesaria para operaciones críticas, se debe deshabilitar siguiendo las guías de Microsoft. Esto elimina el vector de ataque principal para EternalBlue. Se puede hacer vía PowerShell o modificando el registro.
    3. **Eliminar Usuario Creado:** Eliminar la cuenta de usuario javiercastelblanco creada durante la prueba de penetración.
- **Recomendaciones a Corto Plazo:**
    1. **Actualizar/Migrar Windows 7:** El sistema operativo Windows 7 ha llegado al final de su vida útil y ya no recibe actualizaciones de seguridad de Microsoft (*Windows 7 - Microsoft Lifecycle*, 2025). **Es fundamental planificar y ejecutar**

la migración de este equipo a una versión de Windows soportada (Windows 10, Windows 11) o a otro sistema operativo con soporte activo para mitigar riesgos futuros asociados a sistemas obsoletos. Mantener Windows 7 representa un riesgo de seguridad inaceptable a largo plazo.

2. **Segmentación de Red:** Aislar los sistemas que no puedan ser parcheados o actualizados inmediatamente en segmentos de red restringidos para limitar el impacto de un compromiso.
3. **Firewall de Host y Perimetral:** Configurar firewalls para bloquear el tráfico SMB (puerto TCP 445) entrante desde redes no confiables y, si es posible, restringir la comunicación SMB incluso dentro de la red local solo a los hosts que legítimamente la necesiten.

- **Recomendaciones Estratégicas (Largo Plazo):**
    1. **Auditorías de Seguridad Periódicas:** Llevar a cabo pruebas de penetración y auditorías de seguridad internas y externas periódicamente con el fin de detectar y mitigar vulnerabilidades antes de que sean explotadas por atacantes reales.
    2. **Gestión de Vulnerabilidades y Parchado:** Implementar un programa robusto para escanear regularmente la red en busca de vulnerabilidades y asegurar la aplicación oportuna de parches de seguridad en todos los sistemas.
    3. **Monitorización de Seguridad:** Desplegar y mantener sistemas de detección de intrusos (IDS/IPS) y un SIEM (Security Information and Event Management) para detectar actividad sospechosa, como escaneos de SMB o intentos de explotación.

4. **Principio de Menor Privilegio:** Asegurar que los usuarios y servicios operen con los mínimos privilegios necesarios para realizar sus funciones.

Reconocer Las Diferencias Entre un Equipo de Blue Team y el Equipo de Respuesta a Incidentes Informáticos Identificando Sus Funciones y Responsabilidades

Describa Con Sus Palabras Las Diferencias Entre un Equipo Blue Team y un Equipo de Respuesta a Incidentes Informáticos

Tabla 6

Diferencias Entre un Equipo Blue Team y un Equipo de Respuesta a Incidentes Informáticos

Equipo	Funciones	Responsabilidades
Blue Team	**Concienciación y Formación en Seguridad:** Educar a los empleados sobre las mejores prácticas de seguridad y los riesgos existentes. **Defensa Continua:** Implementar, mantener y mejorar las medidas de seguridad de la organización de forma proactiva. **Desarrollo e Implementación de Políticas de Seguridad:** Crear y aplicar las normativas y procedimientos que rigen la seguridad de la información. **Evaluación de Nuevas Tecnologías de Seguridad:** Investigar y probar nuevas herramientas y técnicas defensivas. **Fortalecimiento de Sistemas (Hardening):** Asegurar que los sistemas operativos, aplicaciones y dispositivos de red estén configurados de la manera más segura posible. **Gestión de Vulnerabilidades:** Identificar, evaluar y remediar vulnerabilidades en los activos tecnológicos de la organización. **Monitoreo de Seguridad:** Vigilar constantemente los sistemas y la red en busca de actividades anómalas o posibles amenazas.	Analizar la inteligencia de amenazas para anticipar posibles ataques. Asegurar el cumplimiento de las normativas y estándares de seguridad aplicables. Mantener operativa y actualizada la infraestructura de seguridad (firewalls, IDS/IPS, antivirus, SIEM, etc.). Participar en ejercicios de simulación de ataques (a menudo contra un Red Team) para probar y mejorar las defensas. Preparar a la organización para responder a incidentes (aunque la respuesta directa la lidere el CSIRT). Realizar auditorías de seguridad internas y responder a las externas. Revisar y asegurar la configuración de seguridad de nuevos proyectos o sistemas antes de su puesta en producción.

	Análisis Forense: Recolectar, preservar y analizar evidencia digital para determinar el alcance, la causa y el impacto de un incidente. **Comunicación Durante el Incidente:** Gestionar las comunicaciones internas y externas relacionadas con el incidente (partes interesadas, reguladores, clientes, etc.). **Contención del Incidente:** Tomar medidas inmediatas para limitar la propagación y el impacto de un ataque en curso.	Activar el plan de respuesta a incidentes cuando se detecta o se sospecha un incidente de seguridad. Clasificar y priorizar los incidentes según su gravedad e impacto potencial. Coordinar los esfuerzos de los diferentes equipos técnicos y de negocio durante la respuesta a un incidente.
Respuesta a Incidentes Informáticos (CSIRT)	**Documentación del Incidente:** Registrar todos los detalles del incidente, las acciones tomadas y las lecciones aprendidas. **Erradicación de Amenazas:** Eliminar la causa raíz del incidente y cualquier artefacto malicioso del entorno afectado. **Gestión de Incidentes:** Coordinar y ejecutar todas las fases del ciclo de vida de la respuesta a un incidente (preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas). **Recuperación de Sistemas:** Restaurar de forma segura los datos y sistemas afectados a su estado operativo normal.	Mantener y actualizar el plan de respuesta a incidentes y los playbooks asociados. Mantenerse actualizado sobre las últimas tácticas, técnicas y procedimientos (TTPs) de los atacantes y las mejores prácticas de respuesta. Proporcionar informes detallados post-incidente, incluyendo recomendaciones para prevenir futuros eventos similares. Realizar análisis de malware y de la actividad del atacante.

Nota: Equipo, Funciones y Responsabilidades.

Aunque ambos equipos buscan proteger la organización, el Blue Team se enfoca en la prevención y preparación continua, mientras que el Equipo de Respuesta a Incidentes – CSIRT se enfoca en la acción directa y recuperación durante y después de un incidente. En organizaciones más pequeñas, las mismas personas pueden desempeñar ambos roles, pero las funciones son conceptualmente diferentes.

Evaluar la Pertinencia de Trabajar Con Soluciones de Aseguramiento Como CIS "Center For Internet Security" en un Escenario Real Como Propuesta Del Equipo Blue Team y Argumentar su Uso y Ámbito de Aplicación Para Prevenir Ataques Informáticos

Si Dentro de un Equipo Blue Team le Indican Que Debe Trabajar Con CIS "Center For Internet Security", ¿Usted lo Utilizaría Para Qué Fin?

En una situación como la descrita en el Anexo 5 - Escenario 4, donde se está produciendo de un ataque en tiempo real sobre una máquina Windows 7 y se requiere contenerlo de carácter urgente, mi enfoque con los recursos del CIS (Center for Internet Security) tendría varias facetas, aunque es importante destacar que el gran valor del CIS (*CIS Center for Internet Security*, 2025) radica en la prevención para evitar llegar a este punto crítico.

Como miembro de un equipo Blue Team, utilizaría el CIS, especialmente pensando en cómo su aplicación previa ayudaría en este escenario y cómo se utilizaría después para que este tipo de ataque no vuelva a ocurrir:

Fin y Uso Principal de CIS en el Contexto del Escenario (con foco en la Prevención):

1. **Fortalecimiento Proactivo de la Máquina Windows 7 (Usando Los Puntos de Referencia CIS - Benchmarks):**

- **Fin:** El objetivo fundamental sería haber utilizado los puntos de referencia de CIS (Benchmarks) específicos para el sistema operativo Windows 7 que está siendo atacado antes de que el incidente ocurriera. Estos benchmarks son guías con un gran nivel de detalle, consensuadas por expertos a nivel mundial, que indican exactamente cómo configurar cada aspecto del sistema operativo para cerrarle puertas a los atacantes.
- **Argumento y Ámbito de Aplicación para Prevenir Ataques Informáticos:**

- **Antes del Ataque (Prevención):** Si se hubiera aplicado rigurosamente el punto de referencia CIS correspondiente a esa máquina Windows 7, se habría reducido drásticamente su superficie de ataque. Esto significa desactivar servicios innecesarios que podrían ser explotados, configurar correctamente los permisos para evitar escaladas de privilegios, asegurar las políticas de auditoría para tener mejor visibilidad, entre cientos de otras configuraciones. Muchos ataques prosperan por configuraciones débiles o por defecto, y los Benchmarks ayudan a eliminar estas debilidades.
- **Durante el Ataque (Mejor Posición para Contener):** En el escenario actual, si a la máquina Windows 7 se le hubieran aplicado los puntos de referencia CIS, el análisis exhaustivo que se solicita en el Anexo 5 – Escenario 4 sería sobre un sistema en un estado conocido y más seguro. Esto podría limitar el radio de acción del atacante y facilitaría la identificación de anomalías, ya que se tendría conocimiento de qué configuraciones deberían estar implementadas. La contención sería más sencilla porque el atacante tendría menos herramientas y vías disponibles dentro del sistema.
- **Después del Ataque (Prevención de Recurrencia):** Una vez contenido el ataque, sería obligatorio revisar y volver a aplicar el CIS Benchmark a la máquina Windows 7 afectada y a otras similares para asegurar que la vulnerabilidad CVE-2017-0143 explotada (o cualquier otra cubierta por el benchmark) no pueda ser utilizada de nuevo. Esto es clave para evitar que el mismo incidente, u otro similar, vuelva a suceder.

2. **Establecimiento de una Línea Base de Seguridad y Guía para el Análisis (Usando CIS Controls):**

- **Fin:** Los CIS Controls (*CIS Controls*, 2025) son Controles Críticos de Seguridad que proporcionan un conjunto priorizado de acciones defensivas. Aunque el escenario es de contención, tener un entendimiento de estos controles ayuda a enfocar el "análisis exhaustivo" requerido en el Anexo 5 – Escenario 4.
- **Argumento y Ámbito de Aplicación para Prevenir (y ayudar en la crisis):**
    - **Antes del Ataque (Prevención Estratégica):** Implementar los CIS Controls a nivel organizacional ayuda a construir una defensa robusta en general. Controles como el inventario de hardware y software, la gestión de vulnerabilidades, el control de privilegios administrativos, o la monitorización y defensa de la red son fundamentales. Si estos controles estuvieran maduros, la probabilidad de que este ataque tuviera éxito o pasara desapercibido disminuiría enormemente.
    - **Durante el Ataque (Guía para el Análisis y la Contención):** Mientras se realiza el análisis técnico en la máquina Windows 7 y la red, los CIS Controls sirven como una lista de chequeo mental o formal para identificar qué pudo haber fallado. Preguntas como ¿Falló el control de cuentas?, ¿Hay software no autorizado?, ¿Los logs (cuya configuración robusta es parte de los Benchmarks y apoyada por los Controls) nos están dando la información necesaria? Además, ciertos controles ofrecen orientación sobre cómo segmentar redes o aislar sistemas, lo cual es directamente aplicable a la contención.

- **Después del Ataque (Refuerzo Estratégico):** El análisis post-incidente, informado por los CIS Controls, informará qué defensas a nivel de proceso y tecnología necesitan reforzarse en toda la organización para mejorar la prevención general.

Inmediatamente (Contención): Si bien los recursos del CIS no son herramientas de contención activa como un EDR o un firewall (que debemos usar bajo licencia GPL según el escenario), el conocimiento derivado de ellos (especialmente si los Benchmarks se aplicaron previamente) hace que la máquina Windows 7 sea un entorno más predecible y, por ende, más fácil de analizar y sobre el cual aplicar las herramientas de contención de forma precisa.

A Corto Plazo (Análisis y Erradicación): Los Benchmarks y Controls ayudan a estructurar el análisis técnico, identificando desviaciones de configuraciones seguras que pudieron ser la puerta de entrada o facilitaron el movimiento del atacante.

A Largo Plazo (Prevención y Mejora Continua): Este es el fuerte del CIS. Después de apagar el fuego, los CIS Benchmarks son la guía para reconstruir la máquina Windows 7 (y otras) de forma segura, y los CIS Controls para revisar y fortalecer la estrategia de seguridad global de CyberFort Technologies. El objetivo es que, la próxima vez, el ataque ni siquiera comience o sea neutralizado en sus etapas más tempranas.

Utilizar los recursos del CIS es una señal de madurez para un equipo Blue Team, significa que no solo se apagan los incendios, sino que se trabaja diligentemente para que no se inicien, construyendo defensas basadas en las mejores prácticas de la industria. Y cuando un incidente ocurre, como en este escenario, ese trabajo previo de prevención y estandarización es invaluable para una respuesta y contención más efectivas.

Reconocer las Funciones y Características Principales de un SIEM y su Papel Dentro de la Seguridad Informática de un Escenario Real

Explique y Redacte Las Funciones y Características Principales de lo Que es un SIEM

Tabla 7

Funciones y características principales de un SIEM

Equipo	Funciones Esenciales	Características Clave
SIEM (Security Information and Event Management - Gestión de Información y Eventos de Seguridad)	**Análisis e Investigación (Forense):** Proporcionan herramientas para que los analistas de seguridad investiguen incidentes. Permiten buscar en grandes volúmenes de datos históricos, visualizar patrones de actividad y realizar análisis forenses para entender el alcance de un ataque, su origen y la metodología empleada por el atacante. **Correlación de Eventos:** Utilizando reglas predefinidas y algoritmos de aprendizaje automático identifica relaciones entre eventos aparentemente inconexos que podrían indicar una actividad maliciosa o una brecha de seguridad. **Generación de Alertas y Notificaciones:** Cuando la correlación de eventos identifica una amenaza potencial o una violación de políticas se generan alertas que pueden ser priorizadas según su severidad y notificadas al equipo de seguridad a través de diversos canales (consola del SIEM, correo electrónico, sistemas de ticketing). Esto asegura una respuesta	**Análisis de Comportamiento de Usuarios y Entidades (UEBA):** Funcionalidad avanzada en algunos SIEM que establece líneas base del comportamiento normal de usuarios y dispositivos, y detecta desviaciones que podrían indicar amenazas internas o cuentas comprometidas. **Escalabilidad:** Capacidad para manejar volúmenes crecientes de datos a medida que la organización y su infraestructura tecnológica se expanden. **Inteligencia de Amenazas:** Capacidad para integrar y utilizar feeds de inteligencia de amenazas para enriquecer los datos de eventos y mejorar la detección. **Integración:** Facilidad para integrarse con una amplia variedad de tecnologías y fuentes de datos, así como con otras herramientas de seguridad (como SOAR - Security Orchestration, Automation and Response).

rápida ante incidentes.

Gestión de Cumplimiento y Reportes: Ayudan a automatizar la recopilación de evidencia y la generación de informes necesarios para demostrar el cumplimiento de marcos regulatorios, normativas y estándares de seguridad (ISO 27001, PCI DSS, GDPR, etc.).

Monitorización en Tiempo Real y Paneles de Control (Dashboards): Ofrecen una visualización en tiempo real del estado de la seguridad de la organización a través de paneles de control personalizables. Estos dashboards presentan métricas clave, tendencias de eventos, alertas activas y el estado general de cumplimiento, permitiendo al Blue Team tener una visión general constante.

Normalización y Parseo: Traducen los datos recolectados (múltiples formatos y estructuras) a un formato común y estructurado. Este proceso de normalización es vital para que los datos puedan ser correlacionados y analizados de manera efectiva.

Recopilación y Agregación de Datos (Ingesta de Logs): Recolecta datos de una vasta gama de fuentes dentro de la infraestructura tecnológica como Aplicaciones(Bases de datos, servidores web, aplicaciones corporativas), **Dispositivos de Red (**Firewalls, routers, switches, puntos de acceso inalámbrico), **Fuentes de Inteligencia de Amenazas** (Feeds externos que proveen información sobre indicadores de compromiso (IoCs) actualizados), **Sistemas de Seguridad** (Sistemas de Detección/Prevención de Intrusos

Flexibilidad en la Creación de Reglas: Permite a los equipos de seguridad crear y personalizar reglas de correlación específicas para su entorno y los tipos de amenazas que más les preocupan.

Retención de Logs a Largo Plazo: Almacenamiento seguro y eficiente de los logs durante periodos prolongados para análisis históricos, investigaciones forenses y cumplimiento normativo.

	(IDS/IPS), software antivirus/antimalware, soluciones de Endpoint Detection and Response (EDR), **Sistemas Operativos (**Servidores Windows - Linux, estaciones de trabajo).

Nota: Equipo, Funciones Esenciales y Características Clave.

El Papel del SIEM en el Escenario del Anexo 5 - Escenario 4 (CyberFort Technologies)

En el contexto específico del ataque en tiempo real que enfrenta CyberFort Technologies, y considerando la restricción de usar herramientas GPL, un SIEM basado en soluciones open-source como Wazuh (*Wazuh - Open Source XDR. Open Source SIEM.*, 2025) o el stack ELK - Elasticsearch, Logstash, Kibana (*ELK Stack: Elasticsearch, Kibana, Beats y Logstash*, 2025) adaptado para funciones SIEM jugaría un papel fundamental para el Blue Team en varios frentes:

1. **Detección Temprana y Alerta Inmediata:** Aunque el ataque ya está en curso, un SIEM podría ayudar a identificar la extensión del mismo y cualquier actividad maliciosa nueva o en evolución. Al centralizar los logs de la máquina Windows 7 comprometida y los dispositivos de red relevantes, el SIEM podría correlacionar eventos como:
    - Conexiones de red anómalas desde o hacia la máquina Windows 7 afectada (por ejemplo, comunicación con servidores de Comando y Control - C2).
    - Creación de procesos sospechosos en la máquina Windows 7.
    - Intentos de movimiento lateral desde la máquina Windows 7 comprometida hacia otros sistemas de la red. Las alertas generadas permitirían al Blue Team enfocar sus esfuerzos de contención de manera más precisa.
    - Modificaciones no autorizadas en el registro o archivos críticos del sistema.

2. **Visibilidad Centralizada para el Análisis Exhaustivo:** El escenario demanda un "análisis exhaustivo de lo que está sucediendo a nivel técnico 'sistema operativo, red'". Un SIEM proporciona la plataforma centralizada para este análisis. En lugar de revisar logs manualmente en múltiples sistemas y herramientas dispares (especialmente si se utilizan varias herramientas GPL), el Blue Team podría consultar el SIEM para:
    - Determinar qué cuentas de usuario o sistemas han sido comprometidos.
    - Identificar el vector de ataque inicial (si los logs pertinentes están disponibles).
    - Obtener una cronología de los eventos relacionados con el ataque.
    - Visualizar los flujos de comunicación de la máquina afectada.
3. **Soporte a la Contención del Ataque:** Con la información y las alertas proporcionadas por el SIEM, el Blue Team puede tomar decisiones informadas para "contener el ataque para evitar que se genere más daño a nivel interno de la organización". Por ejemplo:
    - Si el SIEM detecta comunicación con una IP maliciosa, se puede bloquear dicha IP en el firewall.
    - Si se identifica un proceso malicioso específico, se puede proceder a su eliminación en el endpoint.
    - Si se detectan intentos de acceso a otros sistemas, se pueden aislar preventivamente esos sistemas.
4. **Análisis Forense Post-Incidente (Limitado por Herramientas GPL):** Una vez contenido el ataque, el SIEM (con sus logs almacenados) serviría como una fuente invaluable para el análisis post-incidente. Aunque las capacidades forenses de una solución GPL podrían ser más limitadas que las de herramientas comerciales, la información centralizada permitiría al equipo entender mejor cómo ocurrió el ataque, qué

vulnerabilidades fueron explotadas y cómo mejorar las defensas para el futuro. Esto es crucial para aprender del incidente y fortalecer la postura de seguridad de CyberFort Technologies.

5. **Eficiencia del Equipo Blue Team (Incluso con Presupuesto Cero):** Dada la restricción de "no existe presupuesto para hacer uso de herramientas de pago", la eficiencia es clave. Un SIEM open-source, aunque requiere esfuerzo de configuración y mantenimiento, puede multiplicar la efectividad del Blue Team al automatizar la recolección y correlación de logs, liberando tiempo de los analistas para tareas de investigación y respuesta más críticas.

En el escenario de CyberFort Technologies, un SIEM actuaría como el sistema nervioso central para la operación de defensa del Blue Team. Proveería la visibilidad necesaria para entender la naturaleza del ataque en curso sobre la máquina Windows 7, permitiría correlacionar eventos de diversas fuentes para identificar la actividad maliciosa, y facilitaría una respuesta más rápida y efectiva para contener la amenaza, todo ello adaptándose a la restricción de utilizar herramientas de código abierto. Su implementación, incluso con soluciones GPL, representaría un salto cualitativo en la capacidad de detección y respuesta de la organización.

Identificar y Proponer 3 Herramientas Para la Contención de Ataques Informáticos y Validar Que Estas Sean Apropiadas Para su Implementación en un Escenario Real

Defina Por lo Menos 3 Herramientas de Contención de Ataques Informáticos "Hardware o Software", Recuerde Que Las Herramientas de Contención Son Diferentes a Las Herramientas de Detección

Tabla 8

Herramientas de contención de ataques informáticos

Herramienta	Descripción	Aplicabilidad	Validación
pfSense	Es una distribución de software de firewall/router de código abierto basada en FreeBSD (licencia Apache 2.0, que es permisiva y ampliamente aceptada). Se puede implementar en hardware físico o como una máquina virtual.	**Bloqueo de Tráfico Malicioso:** Permite crear reglas para bloquear tráfico hacia y desde direcciones IP, puertos o zonas geográficas específicas que se identifiquen como parte de la infraestructura del atacante. **Interrupción de Conexiones C2:** Puede bloquear las comunicaciones salientes de la máquina comprometida hacia servidores de Comando y Control (C2) conocidos. **Segmentación de Red:** Si el ataque se propaga o para evitar que lo haga, pfSense puede ser utilizado para crear o modificar reglas de firewall que aíslen el segmento de red donde se encuentra la máquina Windows 7 afectada.	Aunque la máquina afectada es Windows 7, la contención a nivel de red es vital para evitar la propagación lateral y cortar la comunicación del atacante. pfSense (*pfSense® - World's Most Trusted Open Source Firewall*, 2024) ofrece estas capacidades sin costo de licencia y es una herramienta robusta y ampliamente utilizada en entornos que requieren soluciones de seguridad de red efectivas.

PowerShell	Es un potente marco de automatización de tareas y gestión de configuración desarrollado por Microsoft, integrado en los sistemas operativos Windows. No es una "herramienta" que se descarga por separado en este contexto, sino una capacidad inherente del sistema operativo.	**Control del Firewall de Windows:** Se pueden utilizar cmdlets de PowerShell para configurar dinámicamente las reglas del Firewall de Windows Defender con seguridad avanzada. Esto permite aislar rápidamente la máquina, bloquear aplicaciones específicas, puertos o direcciones IP directamente en el host afectado. Por ejemplo, se puede crear un script para bloquear toda la conectividad de red excepto para herramientas de análisis específicas que el equipo Blue Team necesite usar. **Desactivación de Interfaces de Red:** Es posible deshabilitar interfaces de red específicas para aislar físicamente (a nivel lógico) la máquina de la red. **Gestión de Procesos y Servicios:** Permite listar, analizar y terminar procesos o servicios maliciosos que se hayan identificado durante la investigación del ataque en tiempo real.	PowerShell (*¿Qué es PowerShell? - PowerShell*, 2024) es una herramienta extremadamente flexible y poderosa disponible en todas las máquinas Windows modernas, lo que la hace perfecta para el escenario donde se requiere una respuesta rápida en un sistema Windows específico sin presupuesto para herramientas adicionales. Permite una contención granular y adaptada a las necesidades inmediatas del incidente.

Wazuh	Es una plataforma de seguridad de código abierto (licencia GPLv2) que funciona como XDR (Extended Detection and Response) y SIEM (Security Information and Event Management). Proporciona detección de amenazas, cumplimiento normativo, monitoreo de integridad y respuesta a incidentes. Para la contención, sus capacidades de "respuesta activa" son cruciales.	**Aislamiento del Host:** Puede ejecutar scripts para modificar las reglas del firewall de la máquina Windows 7 afectada, bloqueando conexiones entrantes y salientes no esenciales, o aislando efectivamente la máquina de la red. **Bloqueo de IPs/Dominios:** Permite bloquear automáticamente direcciones IP o dominios identificados como maliciosos o involucrados en el ataque en curso, tanto a nivel del host como mediante la integración con dispositivos de red. **Desactivación de Cuentas:** En caso de que se identifiquen cuentas de usuario comprometidas, Wazuh (*Wazuh - Open Source XDR. Open Source SIEM.*, 2025) puede ayudar a desactivarlas para evitar su uso malintencionado. **Terminación de Procesos:** Puede identificar y detener procesos maliciosos que estén ejecutándose en la máquina Windows 7 comprometida.	Es ideal para el escenario propuesto porque permite un análisis exhaustivo a nivel de sistema operativo y red en la máquina Windows 7 y tomar acciones de contención directas sobre ella. Al ser de código abierto, cumple con el requisito de no tener costos de licencia.

Nota: Herramienta, Descripción, Aplicabilidad al escenario y Validación.

Conclusiones

La elaboración de este informe técnico ha permitido cristalizar una serie de comprensiones fundamentales desde el enfoque de la ciberseguridad, que trascienden la mera enumeración de herramientas o procedimientos:

1. **La Interdependencia Ofensiva-Defensiva es Clave:** El conocimiento más profundo de la seguridad de un sistema o una organización no surge únicamente de la construcción de defensas, sino de la comprensión íntima de cómo estas pueden ser eludidas o vulneradas. Los ejercicios de Red Team, al simular ataques reales, proporcionan la inteligencia más valiosa para que el Blue Team diseñe, implemente y ajuste controles de seguridad verdaderamente efectivos. Esta simbiosis es esencial para una ciberseguridad madura.
2. **La Ciberseguridad es un Proceso Holístico y Continuo:** No se trata de un estado final, sino de un ciclo constante de evaluación, protección, detección, respuesta y recuperación. Implica la integración de personas (concienciación, ética), procesos (gestión de vulnerabilidades, respuesta a incidentes, cumplimiento de benchmarks CIS) y tecnología (firewalls, SIEM, herramientas de pentesting).
3. **El Marco Legal y Ético Define los Límites de Actuación:** Las capacidades técnicas, por potentes que sean, deben ejercerse con una estricta adherencia a la legalidad (ej. Ley 1273 de 2009) y a los principios éticos profesionales. La ausencia de estos puede convertir al experto en una amenaza, como se discute en los análisis de los anexos. La confianza es un activo primordial en ciberseguridad.
4. **La Práctica Deliberada Conduce a la Maestría Técnica:** La configuración de entornos virtualizados y la ejecución de pruebas de penetración paso a paso, desde el reconocimiento hasta la post-explotación y el reporte, son cruciales para internalizar el

funcionamiento de las vulnerabilidades (como CVE-2017-0143) y la efectividad de las herramientas. Este aprendizaje práctico es insustituible.

5. **La Prevención es Estratégica, la Detección es Táctica, la Respuesta es Crítica:** Si bien el objetivo ideal es prevenir todos los ataques mediante el endurecimiento y la aplicación de controles, la realidad impone la necesidad de detectar actividades anómalas en tiempo real (rol del SIEM) y responder de manera rápida y eficaz para contener el daño y recuperar la operatividad. Un fallo en cualquiera de estas áreas debilita toda la estrategia de seguridad.
6. **El Conocimiento de Herramientas Específicas es un Facilitador, no un Fin en Sí Mismo:** Comprender las capacidades, funcionamiento y utilidad de Nmap, Metasploit, OpenVAS, etc., es vital. Sin embargo, la verdadera pericia radica en saber cuándo y cómo aplicarlas dentro de una metodología estructurada (como las etapas de pentesting) y para alcanzar objetivos estratégicos definidos.

En definitiva, la construcción del conocimiento en ciberseguridad se cimienta en la comprensión teórica robusta, validada y refinada mediante la aplicación práctica y guiada por un fuerte compás ético y legal, reconociendo siempre la naturaleza dinámica y evolutiva de las amenazas y las defensas.

Recomendaciones

Para potenciar la efectividad y madurez de los equipos Red Team y Blue Team, y con base en las lecciones aprendidas y las mejores prácticas evidenciadas en el informe, se plantean las siguientes estrategias y mejoras técnicas:

- **Para Estrategias de Red Team:**
    1. **Automatización de Tareas Repetitivas:** Emplear scripts y herramientas para automatizar fases como el reconocimiento pasivo o el escaneo inicial de vulnerabilidades, permitiendo al equipo centrarse en fases más complejas y creativas del ataque.
    2. **Desarrollo Continuo de TTPs Personalizadas:** Más allá del uso de *exploits* conocidos como EternalBlue, los Red Teams deben invertir tiempo en investigar y desarrollar Tácticas, Técnicas y Procedimientos (TTP) personalizadas que sean menos propensas a ser detectadas por defensas estándar. Esto incluye la creación de *payloads* evasivos, el uso de infraestructura de C2 discreta y la simulación de adversarios específicos (APT).
    3. **Énfasis en la Evasión y Persistencia Avanzada:** Los ejercicios deben enfocarse no solo en obtener el acceso inicial, sino en mantenerlo de forma sigilosa y moverse lateralmente sin ser detectados, utilizando técnicas que eludan EDRs, firewalls de aplicación y otras soluciones de seguridad.
    4. **Integración de Inteligencia de Amenazas (Threat Intelligence):** Utilizar activamente plataformas de inteligencia de amenazas para modelar los ataques basándose en los actores y campañas más relevantes para el sector de la

organización. Esto asegura que los escenarios de prueba sean lo más realistas y pertinentes posible.

5. **Reportes Orientados a la Acción y al Riesgo:** Los informes del Red Team deben ir más allá de la descripción técnica de la vulnerabilidad, traduciendo los hallazgos en riesgos de negocio comprensibles y proporcionando recomendaciones claras y priorizadas que el Blue Team pueda implementar.

- **Para Estrategias de Blue Team:**
    1. **Adopción Proactiva del "Assume Breach Mindset":** Operar bajo la premisa de que la organización ya ha sido comprometida o lo será inevitablemente. Esto impulsa un enfoque en la detección temprana, la respuesta rápida y la limitación del impacto, en lugar de depender únicamente de la prevención perimetral.
    2. **Desarrollo de Capacidades de Threat Hunting:** No depender únicamente de alertas automatizadas. El Blue Team debe dedicar tiempo a la búsqueda proactiva de amenazas (threat hunting) en los logs y datos de telemetría, buscando patrones sutiles que puedan indicar un compromiso.
    3. **Implementación y Optimización Continua del SIEM:** Asegurar que el SIEM esté correctamente configurado con fuentes de logs relevantes de toda la infraestructura (endpoints, servidores, red, aplicaciones), y que las reglas de correlación se ajusten y actualicen constantemente para detectar TTPs modernas. Se debe considerar el uso de UEBA (User and Entity Behavior Analytics) para detectar anomalías.
    4. **Fortalecimiento Basado en CIS Benchmarks y Controles:** Implementar de manera sistemática las guías de *hardenización* de CIS Benchmarks para sistemas

operativos, aplicaciones y dispositivos. Utilizar los CIS Controls como marco para priorizar las defensas.

5. **Planes de Respuesta a Incidentes Detallados y Probados:** Desarrollar *playbooks* específicos para diferentes tipos de incidentes (ransomware, fuga de datos, compromiso de credenciales) y probarlos regularmente mediante simulacros, incluyendo la coordinación con el Red Team para validar su efectividad.

- **Para la Sinergia Red Team & Blue Team (Purple Teaming):**
    1. **Ejercicios Conjuntos Regulares (Purple Teaming):** Fomentar sesiones donde ambos equipos trabajen juntos. El Red Team ejecuta acciones específicas y el Blue Team intenta detectarlas y responder en tiempo real, compartiendo información y mejorando TTPs y controles de forma iterativa.
    2. **Ciclo de Retroalimentación Continuo:** Establecer un mecanismo formal para que los hallazgos del Red Team alimenten directamente las mejoras en las herramientas, procesos y configuraciones del Blue Team, y viceversa (el Blue Team puede informar al Red Team sobre nuevas defensas implementadas).
    3. **Métricas Compartidas de Éxito:** Definir métricas que reflejen la mejora de la postura de seguridad general de la organización como resultado de los esfuerzos combinados, como la reducción del tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR).

Al implementar estas recomendaciones, las organizaciones pueden evolucionar sus capacidades de ciberseguridad, pasando de un enfoque reactivo a una postura más proactiva, resiliente y adaptativa frente a las ciberamenazas.

Referencias Bibliográficas

Alvarez Intriago, V. K. (2018, 1 de abril). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. https://repositorio.uees.edu.ec:8443/server/api/core/bitstreams/f3c021ac-13c7-4506-8d52-ed6b36d8130b/content

Chindrus, C., & Florin Caruntu, C. (2023, 26 de octubre). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. https://www.mdpi.com/2078-2489/14/11/587

CIS Benchmarks®. (2025, 1 de enero). CIS. https://www.cisecurity.org/cis-benchmarks/

CIS Center for Internet Security. (2025, 1 de enero). CIS. https://www.cisecurity.org/

CIS Controls. (2025, 1 de enero). CIS. https://www.cisecurity.org/controls

Código de ética | Copnia. (2015, 1 de enero). Inicio | Copnia. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Convenio Sobre La Ciberdelincuencia. (2001, 23 de noviembre). www.oas.org. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

CSIRT Académico UNAD. (2024, 1 de octubre). Una Mirada a Metodologías Para Pruebas de Penetración en Ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

Customer Guidance for WannaCrypt attacks | MSRC Blog. (2017, 13 de mayo). Microsoft Security Response Center. https://msrc.microsoft.com/blog/2017/05/customer-guidance-for-wannacrypt-attacks/

CVE -CVE-2017-0143. (2017, 1 de enero). CVE -CVE. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Downloads – Oracle VirtualBox. (2025, 1 de enero). Oracle VirtualBox. https://www.virtualbox.org/wiki/Downloads

ELK Stack: Elasticsearch, Kibana, Beats y Logstash. (2025, 1 de enero). Elastic. https://www.elastic.co/es/elastic-stack

Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). (2016, 1 de julio). CCN-CERT - Inicio. https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

handle.exe. (2022, 26 de octubre). live.sysinternals.com - /. https://live.sysinternals.com/

INCIBE. (2019, 4 de julio). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. www.incibe.es. http://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Ley 1581 de 2012 - Gestor Normativo. (2012, 18 de octubre). Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Moreano Jurado, P. J. (2015, 30 de julio). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63). Repositorio Digital USFQ: Página de inicio. https://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Nmap: the Network Mapper - Free Security Scanner. (2025, 1 de enero). Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/

Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html

Normatividad sobre delitos informáticos | Policía Nacional de Colombia. (2025, 1 de enero). Policía Nacional de Colombia. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

pfSense® - World's Most Trusted Open Source Firewall. (2024, 1 de enero). pfSense® - World's Most Trusted Open Source Firewall. https://www.pfsense.org/

Políticas de Privacidad y Condiciones de Uso. (2025, 1 de enero). MINTIC Colombia. https://www.mintic.gov.co/portal/inicio/Seccionesauxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

procexp.exe. (2024, 28 de mayo). live.sysinternals.com - /. https://live.sysinternals.com/

¿Qué es PowerShell? - PowerShell. (2024, 8 de noviembre). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/es-es/powershell/scripting/overview?view=powershell-7.5

Quintero, J. (2020). RedTeam y BlueTeam, Equipos Estratégicos al Interior de Una Organización. [Objeto_virtual_de_Informacion_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/35497

Rajendran, J., Jyothi, V., & Karri, R. (2011, 17 de noviembre). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285-288. IEEE Xplore. https://ieeexplore.ieee.org/document/6081410

Rasool, K. (2024, 15 de agosto). Descripción general de las herramientas de análisis forense de memoria. Paraben Corporation. https://paraben.com/memory-forensics-tools-overview/

smb-vuln-ms17-010 NSE script — Nmap Scripting Engine documentation. (2017, 14 de marzo). Nmap: the Network Mapper - Free Security Scanner. https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html

tcpview.exe. (2023, 11 de abril). live.sysinternals.com - /. https://live.sysinternals.com/

The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community. (2025, 1 de enero). The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community. https://volatilityfoundation.org/

Wazuh - Open Source XDR. Open Source SIEM. (2025, 1 de enero). Wazuh. https://wazuh.com/

Windows 7 - Microsoft Lifecycle. (2025, 1 de enero). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/es-es/lifecycle/products/windows-7

Zambrano Hernández, L. F., Cárdenas Corral, L., Peña Hidalgo, H., & Cárdenas, N. R. (2024, 17 de junio). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guía_para_la_Gestión_y_Clasificación_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus, A. D. (2017, 1 de diciembre). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia. National Open and Distance University UNAD. https://repository.unad.edu.co/handle/10596/17410

Enlace Video Socialización

https://youtu.be/1-TNDed0KMY