CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Marcial Castro Reales

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

Cartagena 03 de diciembre de 2024

Resumen

El presente informe técnico aborda los aspectos clave que contribuyen al desarrollo de estrategias efectivas para equipos de Red Team y Blue Team, destacando su importancia en la identificación y mitigación de vulnerabilidades en sistemas organizacionales. A través de la simulación de ataques y la implementación de defensas robustas, ambos equipos trabajan en conjunto para mejorar la postura de seguridad y garantizar la resiliencia frente a amenazas cibernéticas. Se analiza cómo las pruebas ofensivas del Red Team complementan las respuestas defensivas del Blue Team, y cómo esta colaboración fomenta un ciclo continuo de mejora y adaptación frente a amenazas en evolución.

El informe incluye un conjunto de recomendaciones prácticas orientadas a endurecer los aspectos de seguridad dentro de una organización. Estas estrategias abarcan desde la actualización y gestión de sistemas hasta la implementación de herramientas de contención, monitoreo y detección. Se subraya la importancia de marcos de trabajo como los controles del Center for Internet Security (CIS) para priorizar acciones y optimizar los recursos disponibles. También se recalca la necesidad de establecer políticas claras, segmentar redes, fortalecer los endpoints y garantizar copias de seguridad regulares como pilares de una estrategia de ciberseguridad efectiva.

Palabras claves: integridad, información, seguridad, blueteam, redteam, eventos, riesgos, vulnerabilidad, políticas, ataques, infraestructura, confidencialidad, disponibilidad.

Tabla de contenido

Lista de Figuras

Glosario.

***Backdoor*:** Es una técnica utilizada en seguridad informática que consiste en crear una entrada no autorizada en un sistema informático para permitir el acceso a personas malintencionadas.

***Blue Team*:** Equipo encargado de la seguridad informática de una organización, cuya función es defender los sistemas y prevenir ataques informáticos.

Ciberseguridad: Conjunto de medidas y prácticas destinadas a proteger los sistemas y redes de computadoras contra ataques cibernéticos.

***Cifrado**:* Transformar la información original en un formato ilegible utilizando un algoritmo matemático, de tal manera que sólo las personas que tienen la clave de descifrado pueden leer o acceder a la información original.

Evaluación de vulnerabilidades: Es el proceso en donde los sistemas de seguridad de una organización se analizan y se evalúan con el fin de identificar posibles vulnerabilidades y establecer medidas preventivas.

Exploits: Porción de código o software que aprovecha una vulnerabilidad en un sistema o aplicación para ejecutar acciones maliciosas.

Firewall: Es un sistema o dispositivo que controla la seguridad del tráfico de entrada y salida de información en una arquitectura de red, mediante la configuración de reglas de acceso.

***Framework*:** Son herramientas que proporcionan una estructura para la planificación, implementación, gestión y evaluación de medidas de seguridad de la información en una organización.

Hacking Ético: Práctica de penetración de sistemas y redes de computadoras con el objetivo de encontrar vulnerabilidades y mejorar la seguridad.

Malware: Es cualquier tipo de software diseñado para causar daño o realizar actividades malintencionadas en una computadora o en una red.

***Phishing*:** Técnica para engañar a un usuario para que revele información confidencial o sensible, como contraseñas, números de tarjetas de crédito, o información bancaria.

Políticas de seguridad: Conjunto de directrices y normas que establecen la manera en la que se deben proteger los datos y los sistemas de una organización.

Pruebas de penetración: Evaluación de la seguridad informática mediante la simulación de un ataque para identificar vulnerabilidades.

Red Team: Grupo de expertos en seguridad informática que simulan un ataque informático contra una organización para identificar vulnerabilidades en sus sistemas y procesos de seguridad.

***SIEM*:** Sistema de Gestión de Eventos e Información de Seguridad, que se encarga de recopilar, analizar y notificar información relevante sobre incidencias de seguridad y otros eventos importantes para la infraestructura de una organización.

VPN: Es una tecnología de red que permite establecer una conexión segura y encriptada entre un dispositivo y una red privada a través de Internet.

Introducción.

En el actual panorama digital, las organizaciones enfrentan un creciente número de amenazas cibernéticas que comprometen la integridad, disponibilidad y confidencialidad de sus activos. Este contexto exige el desarrollo de estrategias avanzadas de ciberseguridad que permitan no solo prevenir incidentes, sino también detectar y responder eficazmente a ellos. Los enfoques basados en Red Team y Blue Team se han consolidado como pilares fundamentales para abordar este desafío, ya que combinan perspectivas ofensivas y defensivas para proteger los sistemas frente a ataques cada vez más sofisticados.

Este informe técnico tiene como objetivo explorar los elementos que fortalecen las estrategias de Red Team y Blue Team, destacando cómo la simulación de ataques y el monitoreo continuo permiten identificar vulnerabilidades y desarrollar medidas proactivas. Asimismo, se presentan recomendaciones específicas para endurecer la seguridad en las organizaciones, considerando tanto las herramientas tecnológicas como la implementación de políticas y controles efectivos.

Se analizan las conclusiones derivadas de estas estrategias desde una perspectiva educativa, promoviendo la construcción de conocimiento en ciberseguridad. Este enfoque integral busca proporcionar a las organizaciones una guía práctica para optimizar sus recursos, mitigar riesgos y garantizar una resiliencia efectiva frente a amenazas en constante.

Objetivos.

Objetivo Principal.

Fortalecer las capacidades de ciberseguridad en las organizaciones mediante el desarrollo y análisis de estrategias integradas de Red Team y Blue Team, con el fin de identificar vulnerabilidades, implementar medidas de mitigación y optimizar la respuesta ante incidentes cibernéticos, garantizando la protección de los activos críticos y el cumplimiento de estándares internacionales.

Objetivo Secundarios.

- Analizar las estrategias y herramientas implementadas por los equipos de Red Team y Blue Team para la identificación de vulnerabilidades y diseñar defensas efectivas que fortalezcan la seguridad organizacional.

- Proponer recomendaciones prácticas y técnicas para endurecer los sistemas y redes de las organizaciones, considerando aspectos como la gestión de usuarios, segmentación de redes y aplicación de controles de seguridad.

- Fomentar la construcción de conocimiento en ciberseguridad mediante la integración de enfoques ofensivos y defensivos, promoviendo la adopción de mejores prácticas y marcos internacionales como los controles del CIS.

Desarrollo de informe técnico

1. Aspectos que Aportan al Desarrollo de Estrategias de Red Team & Blue Team.

Los equipos Red Team y Blue team constituyen un elemento importante dentro de la ciberseguridad debido al gran valor que aportan por las características inherentes a sus procedimientos, a continuaciones podemos resaltar algunos de sus aspectos más relevantes:

1.1. Estrategias de Redteam.

El objetivo principal de un Red Team es la verificación o comprobación de la seguridad desde un punto de vista ofensivo es decir un equipo que se encarga de atacar los sistemas con el fin de auditarlos y verificar el nivel de seguridad que tienen. [1]

Cuando hablamos del ejercicio de Red Team nos referimos a una simulación de un ataque dirigido contra una organización, eso significa que vamos a organizar a un grupo de personas profesionales en seguridad informática ya sea que hagan parte del equipo de tecnología de la organización o que sean externos, estos van a comprobar cuál es la posibilidad de lograr acceso a los sistemas e infraestructura tecnológica de la organización y demostrar además cuál sería el impacto a nivel comercial y financiero en caso de que se materializara un ataque informático.

Lo anterior tiene como finalidad mejorar las capacidades tanto de detección cómo de respuesta del equipo de tecnología de la organización ante una situación de ataque dirigido, en otras palabras, estar entrenados para tener una respuesta adecuada en caso de que la materialización

[1] (Jordán, 2021)

de un ataque real.

Para entender cómo funciona el ejercicio del equipo Red Team, se hace necesario conocer las estructuras tecnológicas actuales y su composición a nivel de dispositivos, así como de sistemas de información, de esa manera es posible desarrollar una simulación de ataque dirigido como lo haría un atacante real, el alcance de este ejercicio dependerá de las necesidades actuales de la organización.

1.2. Descripción de características de las fases del Equipo Red Team.

Para llevar a cabo su objetivo principal el Equipo Red Team, debe establecer el desarrollo de un conjunto de fases secuenciales, con las cuales se irán escalando los niveles de la simulación de ataque a los sistemas de información o infraestructura de red objetivo.

Las fases de ataque son un elemento fundamental en las actividades de un equipo Red Team. Estas fases permiten al equipo llevar a cabo un ataque en un entorno controlado, simulando las tácticas y técnicas utilizadas por los atacantes reales.[2] A continuación, se describen las fases genéricas, ver figura 1

[2] (Ciber 4 All Team Tarlogic, 2022)

Figura 1. Fases de simulación de ataque

***Fuente**: (https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/)*

1.2.1. Definición y planificación.

La fase de definición y planificación es crucial en la ejecución de un proyecto de Red Team. En esta etapa, el equipo se enfoca en comprender el entorno objetivo, definir el alcance, los mecanismos necesarios, y planificar la ejecución del proyecto.[3] Una planificación adecuada permite al equipo llevar a cabo el proyecto de manera efectiva y maximizar los resultados obtenidos.

Los procesos que se realizan durante la fase de definición y planificación en un proyecto de Red Team:

En primer lugar, es importante definir el alcance del proyecto de Red Team. Esto conlleva

[3] (Sanchez, 2020)

a determinar cuáles son los sistemas, procesos y aplicaciones que serán objeto de la prueba y qué objetivos específicos se persiguen.

Una vez identificado el alcance, se deben definir los objetivos específicos del proyecto de Red Team. Por ejemplo, los objetivos pueden incluir la obtención de acceso no autorizado a un sistema, identificar fallas o la verificación de la eficacia de las medidas de seguridad.

Para planificar adecuadamente el proyecto de Red Team, es necesario recopilar información detallada sobre el entorno objetivo. Esto puede incluir la recopilación de información sobre la infraestructura de red, los sistemas operativos, las aplicaciones y las políticas de seguridad.

Una vez recopilada la información, el equipo debe definir las herramientas que se implementaran para desarrollar el proyecto de Red Team. Esto puede incluir herramientas de escaneo de vulnerabilidades, exploits, herramientas de ingeniería social y técnicas de *spear-phishing*.

Cuando se hayan definido los objetivos, se ha recopilado la información y se han definido las herramientas, se debe planificar la ejecución del proyecto de Red Team. Esto incluye la definición de un cronograma de trabajo detallado, la asignación de recursos y la concertación de los deberes de cada miembro del equipo.

1.2.2. Reconocimiento externo.

La fase de reconocimiento externo es una de las primeras etapas en la ejecución de un proyecto de Red Team. En esta fase, el equipo se debe enfocar en recopilar información sobre el entorno objetivo desde el exterior, utilizando técnicas de reconstrucción de infraestructura de red y escaneo de puertos para identificar los sistemas, aplicaciones y servicios que estén accesibles en

la red.[4]

Para llevar a cabo esta fase el equipo Red Team debe implementar actividades como: Identificación de dominios, escaneo de puertos, identificar servicios y aplicaciones, identificar las vulnerabilidades del objetivo, por último, el equipo puede intentar identificar a los usuarios y grupos asociados con el entorno objetivo. Esto puede realizarse a través del uso de ingeniería social, como la búsqueda de perfiles de redes sociales asociados con el entorno objetivo.

1.2.3. Compromiso inicial.

La fase de compromiso inicial es la segunda etapa en la ejecución de un proyecto de Red Team y sigue a la fase de reconocimiento externo. En esta etapa, el equipo de Red Team intenta obtener acceso inicial a los sistemas objetivo utilizando técnicas de explotación de vulnerabilidades y de ingeniería social.[5]

En esta fase el equipo utiliza los datos recopilada durante la fase de reconocimiento externo, el equipo identifica las vulnerabilidades presentes en los sistemas objetivo que pueden ser explotadas. Cuando son identificadas las vulnerabilidades, el equipo realiza pruebas de penetración para intentar obtener acceso a los sistemas objetivo. Estas pruebas pueden incluir el uso de herramientas de explotación de vulnerabilidades y técnicas de ingeniería social, como el envío de correos de phishing para confundir a los usuarios y obtener datos de inicio de sesión.

Si el equipo tiene éxito en la explotación de las vulnerabilidades o en la ingeniería social,

[4] (Villar, 2023)
[5] (Mitnick Security Team, 2022)

puede obtener acceso inicial a los sistemas objetivo. Este acceso puede ser de nivel de usuario o administrador, dependiendo del éxito de las pruebas de penetración.[6]

Una vez que se ha obtenido acceso inicial, el equipo trabaja para mantener ese acceso a largo plazo. Esto puede incluir la instalación de backdoors o la modificación de configuraciones para permitir el acceso futuro.

Finalmente, el equipo limpia todas las huellas de su acceso a los sistemas objetivo. Esto puede incluir la eliminación de registros de eventos y la eliminación de archivos que puedan indicar la presencia del equipo de Red Team.

1.2.4. Acceso a la red interna.

En esta fase el equipo de Red Team trabaja para expandir su acceso a la red interna de la organización, con el objetivo final de obtener acceso a los recursos críticos de la red, como los sistemas de bases de datos, servidores de correo electrónico y otros sistemas de producción.

Cuando el equipo ha obtenido acceso inicial a los sistemas objetivo, intentaran escalar los privilegios y obtener acceso a sistemas de mayor nivel dentro de la red. Esto puede estar acompañado de la búsqueda de credenciales de administrador y la explotación de vulnerabilidades para obtener acceso a sistemas más críticos.

Durante esta fase, el equipo de Red Team también identifica otros vectores de ataque que pueden ser explotados para obtener acceso a los sistemas objetivo. Tales como sistemas y dispositivos que tienen vulnerabilidades conocidas o puertos de red que están abiertos y pueden

[6] (Montenegro, 2020)

ser explotados.

Finalmente, el equipo de Red Team llevara a cabo mecanismos para obtener acceso a los recursos críticos de la red, Explorando credenciales de administrador o la explotación de vulnerabilidades para obtener acceso a estos sistemas.

1.2.5. Elevación de privilegios.

En esta fase se establecen actividades para aumentar los permisos y control sobre el sistema comprometido. Cuando el equipo ha logrado acceso a la red interna de la organización, pueden intentar obtener credenciales de usuario más privilegiadas para acceder a sistemas o información crítica.

Para llevar a cabo la elevación de privilegios, los miembros del equipo Red Team pueden utilizar técnicas como la explotación de vulnerabilidades conocidas, la escalada de privilegios de sistemas operativos y aplicaciones, para obtener credenciales de usuario más elevadas.[7]

Cuando se han obtenido permisos elevados, es posible acceder a sistemas y datos sensibles, así como tomar el control de dispositivos y redes. La fase de elevación de privilegios es crítica en el proceso de compromiso de una red, ya que le permite al equipo obtener acceso completo a la red y a los recursos de la organización.

En la fase de elevación de privilegios, el equipo de Red Team busca identificar y explotar vulnerabilidades en los sistemas y aplicaciones, así como evaluar la eficiencia de los procesos de seguridad y la capacitación de los empleados en la organización. Al finalizar esta fase, el equipo de Red Team debe documentar las vulnerabilidades encontradas y proporcionar recomendaciones

[7] (Crosser, 2021)

de seguridad a la organización para mejorar la postura de seguridad.

1.2.6. Reconocimiento interno.

En esta etapa el equipo de Red Team, llevara a cabo operaciones para obtener datos más puntuales sobre la red interna de la organización, sus sistemas y recursos, para identificar posibles vulnerabilidades y puntos de entrada adicionales. Esta fase se lleva a cabo después de que los atacantes hayan logrado acceso a la red interna y hayan elevado sus privilegios.[8]

Durante la fase de reconocimiento interno, los atacantes pueden realizar una serie de mecanismos, como escaneos de puertos y servicios, búsqueda de información de sistemas y usuarios, recopilación de credenciales y contraseñas, y evaluación de la estructura de la red y de las políticas de seguridad.

1.3. Herramientas implementadas según la etapa de pentesting.

1.3.1. Fase de planeación:

se detectan las normas y se obtiene la aprobación de la dirección, lo que se documenta y se establecen los objetivos de las pruebas. Aquí se establece las bases para una prueba de penetración exitosa, aunque no se realizan pruebas reales en esta etapa.

1.3.2. Obtención de la aprobación y autorización formal

Aprobación de la Dirección:

[8] (ArtistCode Team, 2023)

- Se contactó al equipo de dirección y se obtuvo su autorización formal para llevar a cabo un pentesting enfocado en investigar una posible fuga de información en uno de sus servidores.

- Se firmó un Acuerdo de Confidencialidad para proteger la información que se descubra durante el análisis.

Normativas y Cumplimiento:

- El pentesting será realizado en cumplimiento con la normativa interna de seguridad de la empresa y regulaciones aplicables (NIST, ISO 27001).

1.3.3. Definición del alcance y objetivos del pentesting

Alcance:

Máquina objetivo: La prueba se llevará a cabo en la copia del servidor proporcionada por el equipo forense, que contiene la aplicación sospechosa y los logs del sistema.

Sistemas incluidos:

Sistema operativo: Windows (versión a ser confirmada durante el análisis).

Aplicación vulnerable sospechosa identificada por el equipo forense.

Exclusiones: No se realizarán pruebas en sistemas en producción ni en otros entornos que no estén relacionados con la investigación actual.

Objetivos:

Identificar si la aplicación vulnerable permite la fuga de información a través de un exploit.

Validar si el servidor es susceptible a una escalación de privilegios mediante la creación de un usuario administrador.

Demostrar la vulnerabilidad mediante una Prueba de Concepto en la que se cree un usuario administrador con el nombre y apellido del analista.

1.3.4. Evaluación del entorno y recursos disponibles

Recursos Necesarios:

Software y herramientas: Kali Linux, Metasploit, Nmap y OPENVAS

Acceso a la imagen forense proporcionada por el equipo de análisis forense, montada en un entorno seguro (VM).

Asignación de Roles:

Responsable del Pentesting: Marcial Castro, encargado de la ejecución técnica y reporte.

Analista forense: Disponibilidad del equipo forense para consultas y soporte durante la investigación.

Contacto de la organización: Responsable de IT de la empresa como punto de comunicación.

1.3.5. Establecimiento de tiempos y cronograma

Planificación del Tiempo:

- Duración total estimada: 1 semana.

- Cronograma:
  - Día 1: Montaje de la imagen y análisis preliminar.
  - Día 2-3: Escaneo de vulnerabilidades y pruebas de explotación.
  - Día 4: Intento de escalación de privilegios y creación del usuario PoC.
  - Día 5-6: Documentación de resultados y generación del informe final.
  - Día 7: Presentación a la dirección y entrega de recomendaciones.

1.4. Estrategias de Blueteam

El objetivo principal de un equipo Blue Team es proteger la infraestructura de tecnología de la información de una organización contra los ataques cibernéticos, y asegurarse de que los sistemas, datos y recursos estén disponibles, íntegros y confidenciales. El equipo Blue Team es el encargado de monitorear y analizar constantemente la infraestructura de TI para detectar y prevenir posibles ataques.[9]

El equipo Blue Team trabaja en colaboración con el equipo de seguridad informática para establecer medidas y controles de seguridad efectivos, como sistemas de detección y prevención de intrusiones, así como firewalls, sistemas de monitoreo de registros y análisis de vulnerabilidades. También proporcionan la garantía de que se cumplan los requerimientos de seguridad de la organización.

El objetivo final del equipo Blue Team es proteger la organización contra los ataques cibernéticos, minimizando los riesgos de seguridad de la infraestructura de TI y asegurando la continuidad de los negocios. Además, trabajan para mejorar constantemente los procesos de

[9] (Cyber Hub Cybersecurity Check Point, 2023)

seguridad y mantener la organización actualizada frente a las amenazas cibernéticas emergentes.

Dentro de los objetivos específicos del equipo Blue Team podemos resaltar los siguientes:

Definir y aplicar políticas, mecanismos y controles de seguridad para resguardar la red y los sistemas de la organización contra posibles ataques.

Detectar y responder de manera eficiente y efectiva a los intentos de ataque, incluyendo la identificación y mitigación de las vulnerabilidades existentes.

Mejorar continuamente los sistemas y procesos de seguridad de la organización conforme a los resultados destacados en el análisis de incidentes y evaluaciones de seguridad.[10]

1.4.1. Acciones frente a un ataque en tiempo real

Si me encontrara con un ataque en tiempo real en un entorno de producción, la respuesta inicial sería crucial para contener y mitigar el impacto. Aquí está el enfoque técnico y estructurado que seguiría para manejar la situación:

Confirmar y evaluar el alcance del ataque

Verificar rápidamente si el comportamiento sospechoso realmente es un ataque y no una falsa alarma. Esto puede incluir:

Revisar logs en tiempo real (como el Syslog, Event Viewer en Windows, o SIEM) para identificar eventos inusuales como múltiples intentos de inicio de sesión fallidos, creación de usuarios inesperados, o actividad de red anómala.

[10] (Cilleruelo, 2024)

Ejecutar comandos de diagnóstico en los sistemas comprometidos:

- netstat -ano para identificar conexiones sospechosas.
- tasklist para detectar procesos inusuales.

Confirmar que realmente se está produciendo un ataque antes de iniciar una respuesta es crucial para evitar gastar tiempo y recursos en falsas alarmas. No todas las alertas o actividades inusuales son necesariamente maliciosas; pueden deberse a cambios en la configuración, actualizaciones de software o actividades legítimas realizadas por usuarios autorizados. Si se reacciona de forma precipitada ante cada posible incidente sin validarlo, el equipo de seguridad podría verse abrumado, lo que lleva a un uso ineficiente de recursos y puede generar "fatiga de alerta". Esto, a su vez, incrementa el riesgo de que se pasen por alto amenazas reales en el futuro debido a la saturación de eventos que resultan ser benignos.

Al confirmar previamente un ataque, el equipo de respuesta puede enfocarse en contener y mitigar solo los incidentes que representan un peligro real para la organización. Esto permite una respuesta más dirigida y efectiva, maximizando el uso de los recursos disponibles y reduciendo el tiempo de reacción. De esta manera, al priorizar incidentes confirmados, se evita interrumpir operaciones críticas de la organización de forma innecesaria, asegurando que los esfuerzos se concentren en proteger los activos más importantes y en minimizar el impacto de una amenaza genuina.

1.4.2. Aislar el sistema comprometido

Se debe desconectar inmediatamente el dispositivo de la red para evitar la propagación del ataque:

- Desactivar el adaptador de red.
- Utilizar las herramientas de gestión de la red para bloquear el tráfico del sistema comprometido a nivel del firewall o switch.
- Si se tiene acceso físico desconectar el cable de red o conexión inalámbrica.

Aislar un sistema comprometido de la red es una acción crítica para evitar que los atacantes sigan explotando la infraestructura. Si un sistema sigue conectado, los atacantes pueden continuar robando datos sensibles y comprometiendo otros recursos, lo que puede agravar rápidamente la situación. La desconexión del dispositivo detiene de inmediato el flujo de datos hacia el exterior, impidiendo que los atacantes extraigan más información o descarguen herramientas adicionales para consolidar su acceso. Esto es especialmente importante en ataques dirigidos donde los actores de amenazas suelen moverse sigilosamente para no ser detectados.[11]

De igual forma, aislar el sistema previene el movimiento lateral, que es la técnica que usan los atacantes para expandir su acceso desde un equipo inicialmente comprometido a otros sistemas dentro de la red. Al eliminar la conectividad, se limita la capacidad de los atacantes para explorar la red en busca de otras máquinas vulnerables o para escalar privilegios en servidores críticos. Esto proporciona tiempo al equipo de respuesta para analizar el sistema comprometido sin el riesgo de que el ataque se propague, lo que facilita la contención del incidente y minimiza el daño potencial

[11] (Watkins, 2023)

a la organización.

1.4.3. Capturar evidencia para análisis forense

Antes de realizar cualquier acción que pueda alterar el estado del sistema (como apagarlo o reiniciarlo), es vital **capturar evidencia** para un análisis forense posterior:

- Generar un volcado de memoria (RAM) usando la herramienta `volatility`.
- Realizar una imagen completa del disco con la herramienta FTK Imager en Windows.
- Capturar tráfico de red usando herramientas con `Wireshark`.

Capturar la memoria y el disco en su estado actual es una acción muy importante durante un incidente de seguridad, ya que permite preservar evidencia crítica que podría ser alterada si el sistema se apaga o se reinicia. La memoria volátil (RAM) puede contener detalles sobre el ataque, como procesos en ejecución, conexiones de red activas y credenciales temporales utilizadas por el atacante, lo que permite entender cómo accedieron al sistema y qué actividades realizaron. Al capturar una imagen de la memoria antes de que se realice cualquier otra acción, se asegura que todos los datos relevantes se conserven intactos para un análisis forense posterior, ayudando a reconstruir el ataque.[12]

Por otro lado, capturar el disco duro permite obtener una copia exacta del sistema de archivos y configuraciones actuales. Esto incluye información sobre archivos maliciosos, herramientas de explotación o troyanos que los atacantes hayan instalado, así como cualquier

[12] (ENIIT Innova Business School, 2024)

cambio de configuración que hayan realizado en el sistema (como la creación de usuarios o la modificación de privilegios). Analizando tanto la memoria como el disco, los expertos en seguridad pueden determinar el vector de ataque, identificar vulnerabilidades explotadas y rastrear el origen de la intrusión. Esta evidencia es crucial para generar informes detallados, que pueden ser necesarios para tomar decisiones de remediación y, en algunos casos, para cumplir con requisitos legales o regulatorios relacionados con el manejo de incidentes de seguridad.

1.4.4. Realizar análisis en tiempo real

Con la evidencia capturada y el sistema aislado, procedemos a identificar el vector de ataque:

- Buscar procesos anómalos en ejecución, (tasklist) que podrían indicar la presencia de malware o shells remotos.
- Examinar archivos de configuración (registros Windows) para detectar creación de usuarios o tareas programadas sospechosas.
- Utilizar herramientas como netstat y lsof para analizar conexiones de red activas que podrían estar indicando la presencia de un canal de comunicación controlado por el atacante.

Realizar un análisis rápido en tiempo real durante un ataque es crucial para identificar las herramientas y tácticas que el atacante está utilizando en el momento. Esto permite detectar signos evidentes de explotación, como procesos sospechosos, conexiones de red inusuales o modificaciones no autorizadas en los sistemas, que son indicativos de la actividad del atacante. Al identificar estas herramientas (como shells remotas, malware o programas de escalada de

privilegios), los equipos de seguridad pueden determinar el alcance del ataque, la persistencia de los intrusos en el sistema y el tipo de daños que podrían estar causando. Además, este análisis permite reconocer si se están utilizando técnicas comunes, como la movilidad lateral o la creación de cuentas de usuario no autorizadas, lo cual es vital para responder de manera eficaz.

Un análisis rápido también ayuda a guiar la respuesta inmediata de forma más enfocada y precisa. Al conocer las tácticas y herramientas del atacante, el equipo de seguridad puede implementar medidas específicas, como bloquear puertos, eliminar procesos maliciosos, aislar sistemas comprometidos o cortar las conexiones de red utilizadas para exfiltrar datos. Esta acción rápida limita el impacto del ataque, evita su propagación y facilita la contención del incidente, reduciendo así el tiempo que los atacantes tienen para causar más daño. La capacidad de actuar rápidamente, con base en un análisis en tiempo real, puede marcar la diferencia entre una respuesta exitosa y una brecha de seguridad que se extiende.

1.4.5. Contención y remediación

Basado en los hallazgos anteriores:

- **Eliminar los procesos maliciosos** (`taskkill /PID` en Windows).
- **Bloquear direcciones IP sospechosas** en el firewall.
- **Revocar accesos** y contraseñas comprometidas de inmediato.
- **Parchar** cualquier vulnerabilidad explotada (actualizar software vulnerable).

La contención es una medida urgente y crítica para detener inmediatamente la actividad del atacante y evitar que cause más daño mientras se trabaja en una solución a largo plazo. Consiste en aislar el sistema comprometido, cortar las conexiones de red maliciosas, bloquear el acceso no autorizado y limitar la capacidad del atacante de moverse lateralmente dentro de la red. La contención tiene como objetivo reducir el impacto del ataque, evitar la exfiltración de datos y detener cualquier actividad destructiva, como la instalación de malware o la escalada de privilegios. Sin esta acción inmediata, el atacante podría seguir manipulando los sistemas, lo que aumentaría la complejidad y el costo de la recuperación.

A pesar de que la contención es esencial para mitigar el daño en el corto plazo, no es una solución definitiva. Una vez contenida la amenaza, es necesario implementar una remediación a largo plazo que aborde las vulnerabilidades explotadas por el atacante. Esto puede incluir la actualización de sistemas, el fortalecimiento de las políticas de seguridad, la eliminación de herramientas maliciosas y la corrección de brechas en la infraestructura de red. Además, la remediación también implica realizar un análisis forense completo para identificar el origen del ataque, las tácticas utilizadas y los datos comprometidos, lo que permitirá implementar medidas preventivas que aseguren que ataques similares no ocurran en el futuro.

1.4.6. Notificación y comunicación

La comunicación oportuna durante un incidente de seguridad es importante para garantizar que las partes involucradas en los procesos de la compañía, tanto internas como externas, estén al tanto de la situación y puedan tomar las acciones necesarias. Esto incluye informar a la alta dirección, a los equipos de TI, seguridad, administración y otros departamentos relevantes dentro

de la organización, de manera que puedan coordinar la respuesta y colaborar para mitigar el impacto del ataque. Así mismo, una comunicación clara y rápida asegura que se pueda tomar una decisión informada sobre el alcance de la brecha y las medidas inmediatas que se deben implementar para contenerla, como la desconexión de sistemas comprometidos o el aislamiento de la red.

1.5. Aspectos legales

1.5.1. Marco legal en Colombia, sobre la protección de la información

Ley 1273 de 2009: Delitos Informáticos

En esta ley del 2009 se agrega el apartado jurídico "la protección de la información y de los datos"[13]. Surge como necesidad para emitir sanciones a infracciones de índole informático, lo anterior en búsqueda de brindar protección a los sistemas de información y a la data, dentro de sus puntos principales podemos resaltar:

- Se castiga al individuo que infrinja el acceso, de manera no autorizada a un sistema de información resguardado con medidas de seguridad.
- Penaliza la intervención sin autorización en una transmisión de datos o comunicaciones privadas.
- Se sanciona a quien destruya, altere o inutilice información contenida en un sistema informático.
- Quien introduzca, difunda o emplee programas destinados a afectar sistemas

[13] **Fuente especificada no válida.**

informáticos o datos ajenos es sancionado.

- Penaliza la creación de sitios web con la intención de obtener información de manera fraudulenta (phishing).

1.5.2. Ley 1581 de 2012: Protección de Datos Personales

Esta ley es popularmente reconocida como habeas data, esta describe el control que se debe implementar en el tratamiento de la información personal, plasmando directrices y derechos sobre los dueños de los datos, así como deberes para quienes custodian dicha información, dentro de sus puntos principales podemos resaltar:

- Cada individuo tendrá el derecho tener acceso, actualizar o modificar la data que se guarde sobre él en bases de datos.
- Los datos personales solo pueden ser gestionados si el titular ha dado su autorización de manera anticipada, explícita y con pleno conocimiento.
- Derecho a solicitar prueba del consentimiento, a revocar la autorización, a acceder a la información y a solicitar la corrección de datos incorrectos o incompletos.
- La ley establece responsabilidades específicas para las personas o entidades que recogen y procesan los datos personales.

1.5.3. Decreto 1377 de 2013

Este decreto ayuda a que las organizaciones sigan correctamente la ley de protección de

datos personales, asegurando que las personas tengan control sobre cómo se manejan sus datos y que las empresas tomen medidas para proteger esta información.

1.5.4. Decreto 886 de 2014

Este decreto establece las reglas para la creación y manejo del Registro Nacional de Bases de Datos en Colombia. Este registro es una plataforma donde todas las empresas y organizaciones que manejan o recolectan datos personales deben inscribirse. La responsabilidad de administrar este registro recae en la Superintendencia de Industria y Comercio (SIC).

2. Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.

2.1. Mantener actualizaciones al día.

La actualización y parcheo de seguridad son medidas fundamentales para proteger un sistema contra ataques, especialmente en entornos Windows. Los fabricantes de sistemas operativos, sistemas de información y apps, liberan parches de seguridad para corregir vulnerabilidades tan pronto como se descubren, ya que estas fallas podrían ser explotadas por ciberdelincuentes a fin de conseguir acceso, lanzar scripts maliciosos o escalar privilegios. Mantener el sistema operativo Windows actualizado garantiza que las últimas correcciones estén aplicadas, reduciendo así la superficie de ataque disponible. Esto es particularmente crucial para vulnerabilidades críticas que permiten la explotación remota, como las que comúnmente se utilizan en herramientas como Metasploit.[14]

[14] (FORLOPD, 2024)33

No solo el sistema operativo debe mantenerse al día, sino también todas las aplicaciones instaladas en el equipo. Muchas veces, los atacantes aprovechan programas desactualizados que contienen fallas conocidas para introducir malware o abrir puertas traseras. Herramientas de productividad, navegadores, y software de terceros son objetivos frecuentes debido a su uso generalizado. Al implementar un programa de gestión de actualizaciones tanto para el sistema como para las aplicaciones, se reduce la probabilidad de que los atacantes puedan explotar vulnerabilidades para comprometer la seguridad del sistema, logrando así un entorno más robusto y protegido frente a posibles ataques.

2.2. Controles de acceso y gestión de usuarios.

La configuración y gestión de usuarios es una práctica crucial para mitigar los riesgos de escalamiento de privilegios y accesos no autorizados. Desactivar la cuenta de administrador predeterminada en sistemas Windows y crear cuentas con privilegios mínimos asegura que los atacantes no puedan aprovechar credenciales predeterminadas para comprometer el sistema. Al limitar el acceso de administrador solo a quienes realmente lo necesitan, se reduce el riesgo de que una cuenta comprometida pueda ser utilizada para realizar cambios críticos en la configuración del sistema. Esto involucra limitar los derechos administrativos a personal técnico específico y no a usuarios generales, minimizando así la exposición.

Aplicar el principio de privilegio mínimo es importante para restringir el acceso a solo aquellos recursos que los usuarios necesitan para realizar su trabajo. Esto se complementa con políticas de contraseñas robustas que deben ser actualizadas regularmente, ya que contraseñas

débiles o no renovadas son una de las principales causas de accesos no autorizados. Para fortalecer aún más la seguridad, habilitar la autenticación multifactor en todas las cuentas, especialmente las de administrador, proporciona una capa adicional de protección. El uso de MFA asegura que incluso si un atacante obtiene una contraseña, no podrá acceder sin el segundo factor de autenticación, lo que reduce significativamente el riesgo de intrusión.

2.3. Fortalecimiento de servicios y aplicaciones.

Este punto es fundamental para reducir la superficie de ataque en un sistema Windows. Uno de los primeros pasos es desinstalar aplicaciones innecesarias y deshabilitar servicios que no se utilizan, ya que estos pueden ser aprovechados por los atacantes para obtener acceso al sistema. Aplicaciones y servicios sin uso o mal configurados son vectores potenciales que los atacantes pueden explotar mediante vulnerabilidades conocidas o configuraciones por defecto. Al eliminar estos posibles puntos de entrada, se reduce considerablemente la posibilidad de que un atacante comprometa el sistema.

Adicionalmente, configurar el Firewall de Windows de forma adecuada es crucial para limitar las conexiones entrantes y salientes. Bloquear puertos no utilizados, especialmente aquellos que son frecuentemente objetivo de exploits (como 445 para SMB, 135 para RPC y 3389 para RDP), ayuda a prevenir ataques como la propagación de malware o el acceso remoto no autorizado. Para proteger aún más el entorno, se recomienda utilizar AppLocker o Windows Defender Application Control para restringir la ejecución de aplicaciones y scripts no autorizados. Estas herramientas permiten definir políticas que solo permiten la ejecución de software aprobado, lo que impide que los atacantes ejecuten código malicioso o scripts que puedan comprometer el

sistema, elevando significativamente el nivel de seguridad.

2.4. Políticas de seguridad.

El endurecimiento del sistema y la implementación de políticas de seguridad son importantes para proteger los equipos Windows frente a ataques sofisticados. Utilizar un endpoint moderno con protección avanzada contra amenazas (ATP) permite detectar y bloquear actividades maliciosas en tiempo real. Las soluciones ATP están diseñadas para identificar comportamientos anómalos y responder automáticamente a posibles amenazas, lo que reduce el tiempo que un atacante puede permanecer en un sistema comprometido. Esta capa de protección adicional complementa las defensas tradicionales, ya que ATP puede detectar amenazas más avanzadas que podrían pasar desapercibidas, como movimientos laterales y técnicas de evasión de malware.[15]

La configuración de políticas de seguridad de grupo (GPO) refuerza el entorno al restringir ciertas actividades que los atacantes suelen aprovechar. Por ejemplo, limitar la creación de usuarios y la ejecución de scripts reduce el riesgo de escalación de privilegios y la ejecución de código no autorizado. Asimismo, deshabilitar macros en aplicaciones de Microsoft Office es una medida preventiva para evitar que documentos maliciosos puedan ejecutar código al abrirse. Por otro lado, activar el Control de Cuentas en un nivel estricto asegura que cualquier intento de realizar cambios críticos en el sistema requiera una autorización explícita del usuario, lo que complica los intentos de los atacantes de escalar privilegios y tomar control del sistema sin ser detectados.

2.5. Monitoreo de la infraestructura.

[15] (Martinez, 2024)

El monitoreo y detección son componentes fundamentales para identificar y responder de forma rápida a posibles incidentes de seguridad. Implementar un sistema de detección de intrusiones (IDS/IPS) permite detectar patrones sospechosos en el tráfico de red y en los sistemas, como intentos de escalamiento de privilegios, conexiones a puertos inusuales o comportamientos anómalos. Estas herramientas pueden activar alertas en tiempo real, lo que permite a los equipos de seguridad responder de inmediato antes de que un atacante logre su objetivo. La detección temprana es clave para contener amenazas y evitar que se conviertan en incidentes mayores que puedan comprometer la seguridad de la organización.

Configurar logs detallados en todos los sistemas y asegurarse de que el Event Viewer en Windows esté capturando eventos críticos proporciona visibilidad sobre lo que está sucediendo en la infraestructura. Los registros deben incluir información como intentos de inicio de sesión fallidos, creación de usuarios inesperados y accesos sospechosos, ya que estos son indicadores comunes de intentos de ataque. Para gestionar y analizar esta gran cantidad de datos de manera eficiente, es fundamental utilizar herramientas de SIEM, el cual permite correlacionar eventos en línea, evidenciando comportamientos que podrían sugerir una brecha de seguridad en progreso, lo que ayuda a las organizaciones a responder de forma proactiva y reducir el impacto de los ataques.

2.6. Protección de la red.

El endurecimiento de la red es crucial para contener posibles ataques y limitar el alcance de un intruso si logra comprometer un sistema. Una de las mejores prácticas es la segmentación de la red, que separa los activos críticos en segmentos distintos y controla el flujo de tráfico entre ellos. Esto significa que, en caso de que un atacante comprometa un sistema en un segmento menos crítico, le será mucho más difícil acceder a otros sistemas, como servidores que contienen

información sensible o aplicaciones empresariales. Al limitar el movimiento lateral, se reduce drásticamente la capacidad del atacante para expandir su alcance dentro de la red y comprometer otros sistemas.

Así mismo, es vital proteger el acceso remoto mediante el uso de VPNs y conexiones seguras en lugar de exponer servicios como RDP directamente a Internet, ya que estos son objetivos comunes de ataques de fuerza bruta y exploits. Configurar un conjunto de listas de controles de accesos en routers y switches permite limitar el tráfico entre segmentos de la red, de modo que solo los activos de información y cuentas autorizadas puedan comunicarse con sistemas específicos. Estas medidas no solo mejoran la seguridad del entorno, sino que también permiten un control más granular sobre quién puede acceder a qué recursos, reduciendo así el riesgo de que un atacante logre moverse libremente una vez que ha penetrado la red.[16]

2.7. Respaldo y plan de desastres.

Las copias de seguridad regulares y actualizadas son una de las defensas más efectivas contra la pérdida de datos causada por ataques, como el ransomware. Es fundamental asegurarse de que estas copias de seguridad no solo sean frecuentes sino también almacenadas en ubicaciones seguras y desconectadas de la red principal, lo que evita que los atacantes las comprometan en caso de que logren acceder al entorno.[17] Al mantener estas copias aisladas, incluso si un sistema es atacado, los datos críticos pueden restaurarse sin ceder al chantaje de los atacantes. Además, realizar verificaciones periódicas de estas copias garantiza que sean funcionales y que se puedan

[16] (Instituto Americano, 2023)
[17] (Seguridad de Microsoft, 2024)

recuperar rápidamente en caso de un incidente.

Por otro lado, se debe contar con un plan de respuesta ante incidentes bien desarrollado es esencial para gestionar eficazmente un ataque cuando ocurre. Este plan debe incluir procedimientos detallados para contener la amenaza, mitigar el daño, y restaurar la operatividad. Realizar simulaciones periódicas ayuda a los equipos a familiarizarse con el proceso y a mejorar su capacidad de reacción bajo presión, lo que reduce el tiempo de inactividad y el impacto general de un ataque real. Asimismo, configurar puntos de restauración en Windows proporciona una opción rápida para revertir el sistema a un estado anterior en caso de una infección o cambios maliciosos, acelerando así la recuperación y minimizando la interrupción del negocio.

3. Conclusiones para la construcción del conocimiento desde el enfoque de la ciberseguridad.

3.1. El conocimiento como base para la ciberseguridad organizacional

La ciberseguridad efectiva depende de una comprensión profunda y multidisciplinaria del conocimiento organizacional. Este debe ser abordado como un sistema dinámico e interconectado, en el que interactúan individuos, procesos, tecnología y estructuras sociales. El conocimiento no solo habilita la detección y mitigación de amenazas, sino que también guía la formulación de estrategias adaptativas que responden al entorno cambiante.

3.2. La importancia del enfoque fenomenológico.

La construcción del conocimiento en ciberseguridad debe trascender los aspectos puramente técnicos para integrar dimensiones sociales, culturales, organizativas y cognitivas. Este enfoque permite abordar la ciberseguridad como un fenómeno complejo y contextual, adaptado a las necesidades y características únicas de cada organización. Asimismo, fomenta una visión sistémica que incorpora tanto las capacidades individuales como las colectivas.[18]

3.3. Adaptación como proceso continuo de construcción del conocimiento.

La rápida evolución de las amenazas cibernéticas requiere que las organizaciones cultiven una capacidad constante de "desaprender" prácticas obsoletas y "reaprender" nuevos enfoques. Este ciclo de renovación asegura que el conocimiento organizacional siga siendo relevante y efectivo. Además, refuerza la importancia de una cultura organizacional orientada al aprendizaje, la experimentación y la mejora continua.

3.4. La inteligencia colectiva como motor de la resiliencia organizacional.

La construcción del conocimiento en ciberseguridad debe apoyarse en redes de colaboración tanto internas como externas. Internamente, la cooperación entre equipos y niveles jerárquicos fortalece las capacidades colectivas para anticipar, identificar y responder a amenazas. Externamente, el intercambio de información y recursos con otras organizaciones y comunidades de ciberseguridad amplifica la capacidad de respuesta ante amenazas globales.

[18] (Sallos, Garcia Perez, & A. D. Bedford, 2020)

3.5. El rol que juega la tecnología en la promoción de conocimiento estratégico.

Herramientas como el estudio de la big data, la emergente inteligencia artificial, asi como los sistemas colaborativos desempeñan un papel clave en la consolidación y el procesamiento de información crítica. Estas tecnologías permiten identificar patrones, anticipar amenazas emergentes y diseñar estrategias informadas, contribuyendo a una toma de decisiones más robusta y basada en evidencia.

3.6. Hacia un marco epistemológico sólido en ciberseguridad.

La construcción del conocimiento en este campo debe basarse en principios epistemológicos que integren tanto el conocimiento explícito (codificado y formal) como el tácito (práctico y experiencial). Este equilibrio permite que las organizaciones desarrollen capacidades tanto operativas como estratégicas, asegurando su sostenibilidad en entornos altamente dinámicos y competitivos.

La construcción del conocimiento en ciberseguridad exige un enfoque integral que articule dimensiones técnicas, sociales y organizacionales. Adoptar un marco fenomenológico, dinámico y colectivo no solo fortalece la capacidad de las organizaciones para protegerse de amenazas actuales, sino que también las prepara para abordar futuros desafíos con resiliencia e innovación. Este enfoque fomenta una cultura de aprendizaje continuo y colaboración, donde el conocimiento se transforma en el recurso estratégico más importante para la seguridad y el éxito organizacional.

Conclusión

La implementación de estrategias efectivas de Red Team y Blue Team es fundamental para proteger a las organizaciones frente a un panorama cibernético cada vez más complejo y dinámico. Estos equipos, al trabajar de manera colaborativa, permiten identificar vulnerabilidades críticas y diseñar respuestas proactivas que mitigan los riesgos asociados a ciberataques. Las pruebas de penetración realizadas por los Red Teams, combinadas con las defensas activas de los Blue Teams, crean un ciclo continuo de mejora que fortalece la resiliencia organizacional frente a amenazas emergentes.

Las recomendaciones propuestas en este informe, como el endurecimiento de los sistemas mediante la actualización constante, la segmentación de redes y la implementación de controles de seguridad, son esenciales para optimizar las defensas de la infraestructura de TI. De igual manera, se resalta la importancia de marcos de trabajo como los controles del Center for Internet Security (CIS), que proporcionan un enfoque estructurado y basado en las mejores prácticas para gestionar y reducir los riesgos cibernéticos.

La adopción de un enfoque integral que combine la simulación de ataques y la defensa continua contribuye al fortalecimiento de la ciberseguridad organizacional. Este enfoque no solo permite prevenir incidentes, sino que también asegura una respuesta efectiva a los ataques, promoviendo un ciclo de aprendizaje continuo y la adaptación a un entorno de amenazas en constante evolución. La ciberseguridad es un proceso dinámico que debe ser abordado de manera colaborativa, con una visión a largo plazo y un compromiso constante con la mejora y la educación.

Recomendaciones.

Explorar nuevas tecnologías de Seguridad para estar al tanto de las técnicas emergentes, así como las herramientas de seguridad para evaluar su aplicabilidad en las operaciones de los equipos Red Team y Blue Team en entornos de infraestructuras tecnológicas organizacionales.

En la dinámica y siempre cambiante paisaje de la seguridad informática, es imperativo que los equipos Red Team y Blue Team estén constantemente explorando y evaluando las innovaciones en tecnologías de seguridad. Esta exploración no solo implica conocer las últimas tendencias, sino también entender cómo estas tecnologías pueden optimizar las operaciones y fortalecer la postura de seguridad en la infraestructura de nube

Realizar evaluaciones periódicas de los objetivos del equipo Red Team y Blue Team, ajustándolos según la evolución de las amenazas y la infraestructura tecnológica.

Destacando la importancia de la adaptabilidad y la alineación constante de los objetivos de los equipos Red Team y Blue Team con el entorno cambiante de amenazas y la infraestructura de nube. La realización de evaluaciones periódicas garantiza que los equipos estén en sintonía con los riesgos actuales y futuros, permitiendo ajustes estratégicos y tácticos para mantener un alto nivel de seguridad.

Establecer mecanismos de monitoreo continuo para rastrear la evolución del panorama de amenazas informáticas. Esto implica mantener actualizadas las tácticas, técnicas y procedimientos utilizados por los actores malintencionados y comprender cómo estas amenazas pueden afectar específicamente a la infraestructura en la nube, tener en cuenta que el monitorio no solo implica la

observación de amenazas externas, sino también la identificación temprana de posibles vulnerabilidades en la infraestructura tecnológica. Esto permite a los equipos Red Team y Blue Team abordar proactivamente las debilidades antes de que sean explotadas por los ciberdelincuentes.

Incorporar auditorias de seguridad periódicas de terceros para obtener una perspectiva externa y objetiva de los riesgos en la infraestructura tecnológica, garantizando una evaluación completa, el alcance de estas evaluaciones debe ser integral, abarcando diversos aspectos de la infraestructura tecnológica, como configuraciones de seguridad, gestión de accesos, protocolos de cifrado y cualquier otro elemento relevante. Una vez completadas las evaluaciones, el equipo de seguridad interna debe analizar detalladamente los resultados proporcionados por los evaluadores externos. Esto implica comprender las vulnerabilidades identificadas, su gravedad y las posibles medidas correctivas.

Organizar simulacros periódicos de crisis para poner a prueba la capacidad de respuesta ante situaciones de emergencia y mejorar la preparación del equipo para enfrentar amenazas en tiempo real. La realización de simulacros de crisis implica la organización de eventos planificados y controlados que simulan situaciones de emergencia o incidentes de seguridad cibernética. El objetivo principal es evaluar y mejorar la capacidad de respuesta del equipo ante amenazas inesperadas. Se deben llevar registros detallados durante el simulacro para evaluar el desempeño individual y colectivo del equipo. Estos registros ayudarán a identificar áreas de mejora y a ajustar los procedimientos y protocolos de respuesta. Después de completar el simulacro, es importante realizar un análisis posterior.

Bibliografía

Cyber Writes Team. (22 de 6 de 2023). *What is Metasploit: Tools, Uses, History, Benefits, and Limitations*. Obtenido de Cyber Writes Blog: https://cybersecuritynews.com/what-is-metasploit/

ArtistCode Team. (2023). *Red Team*. Recuperado el 29 de 11 de 2024, de ArtistCode Blog: https://www.artistcode.net/post/red-team

Ciber 4 All Team. (2022). *Controles CIS: las mejores prácticas en ciberseguridad*. Recuperado el 21 de 11 de 2024, de Tarlogic Security : https://www.tarlogic.com/es/blog/controles-cis-ciberseguridad/

Ciber 4 All Team Tarlogic. (2022). *Red Team: El poder de la seguridad ofensiva*. Recuperado el 29 de 11 de 2024, de Tarlogic Blog: https://www.tarlogic.com/es/blog/red-team-seguridad-ofensiva/

Cilleruelo, C. (2024). *Conoce los objetivos y tareas del Blue Team*. Recuperado el 29 de 11 de 2024, de Keepcoding Tech School: https://keepcoding.io/blog/objetivos-y-tareas-del-blue-team/

Congreso de la República de Colombia. (2023). *Ley 1581 de 2012*. Recuperado el 29 de 11 de 2024, de Funcion Publica de Colombia: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Crosser, A. (2021). *Red Team Privilege Escalation*. Recuperado el 29 de 11 de 2024, de Praetorian: https://www.praetorian.com/blog/red-team-privilege-escalation-rbcd-based-privilege-escalation-part-2/

Cyber Hub Cybersecurity Check Point. (2023). *What is a Blue Team?* Recuperado el 29 de 11 de 2024, de Check Point Software Technologies Ltd: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-blue-team/

Diaz, M. A. (2024). *Optimización de un SIEM para la Detección de Amenazas en Tiempo Real*. Recuperado el 21 de 11 de 2024, de NOVARED Blog Ciberseguridad: https://www.novared.net/optimizacion-de-un-siem-para-la-deteccion-de-amenazas-en-tiempo-real/

ENIIT Innova Business School. (2024). *Informática Forense: Las herramientas y técnicas que debes dominar*. Recuperado el 20 de 11 de 2024, de Campus Ciberseguridad Blog: https://www.campusciberseguridad.com/blog/item/189-informatica-forense-herramientas-tecnicas-deber-dominar

FORLOPD. (2024). *Actualizaciones de Software y Parches de Seguridad: Por qué son cruciales*. Recuperado el 20 de 11 de 2024, de FORLOPD Blog Ciberseguridad: https://forlopd.es/actualizaciones-de-software-y-parches-de-seguridad-por-que-son-cruciales/

Instituto Americano. (2023). *Asegurando las redes*. Recuperado el 21 de 11 de 2024, de Instituto Americano de Formación Blog Seguridad: https://www.institutoamericano.es/asegurando-las-redes-conceptos-de-la-lista-de-control-de-acceso-acl/

Jordán, J. (2021). *Red Team: identificando nuestras vulnerabilidades*. Recuperado el 29 de 11 de 2024, de Global Strategy: https://global-strategy.org/red-team-la-importancia-de-identificar-nuestras-vulnerabilidades/

Martinez, E. (2024). *Detecta comportamientos anómalos con VMware Carbon Black*. Recuperado el 21 de 11 de 2024, de AO DATA CLOUD Blog: https://aodatacloud.es/blog/detecta-comportamientos-anomalos-con-vmware-carbon-black/

Mitnick Security Team. (2022). *Red Teaming Everything You Need to Know*. Recuperado el 29 de 11 de 2024, de Mitnick Security Consulting LLC: https://www.mitnicksecurity.com/red-teaming

Montenegro, I. (2020). *Red Teaming: Ataca tus propias vulnerabilidades y mejora tu ciberseguridad*. Recuperado el 29 de 11 de 2024, de GB Advisors Tech Blog: https://www.gb-advisors.com/es/red-teaming-ataca-tus-propias-vulnerabilidades-y-mejora-tu-ciberseguridad/

Moraguez, E. R. (2023). *Firewalls: Cómo Funcionan y Cómo Configurarlos para una Protección Óptima*. Recuperado el 21 de 11 de 2024, de LovTechnology Articulo Ciberseguridad: https://lovtechnology.com/firewalls-como-funcionan-y-como-configurarlos-para-una-proteccion-optima/

Robb, D. (2024). *23 Top Open Source Penetration Testing Tools*. Obtenido de EsecurityPlanet: https://www.esecurityplanet.com/applications/open-source-penetration-testing-tools/

Sallos, M. P., Garcia Perez, A., & A. D. Bedford, D. (2020). *Strategy and organisational cybersecurity: a knowledge-problem perspective*. Recuperado el 29 de 11 de 2024, de Journal of Intellectual Capital: https://www.researchgate.net/publication/335624164_Strategy_and_organisational_cybersecurity_a_knowledge-problem_perspective

Sanchez, M. V. (2020). *Seguridad ofensiva en Windows: Fundamentos de Red Team*. Recuperado el 29 de 11 de 2024, de UNIVERSIDAD DE CASTILLA LA MANCHA: https://mcsi.uclm.es/wp-content/uploads/2021/05/TFM_MarioVegaSanchez.pdf

Seguridad de Microsoft. (21 de 11 de 2024). *Plan de recuperación de ataques de ransomware*. Obtenido de Microsoft Learn Challenge: https://learn.microsoft.com/es-es/security/ransomware/protect-against-ransomware-phase1

Villar, E. (2023). *Cómo reforzar la seguridad de su empresa con pruebas de Red Team*. Recuperado el 29 de 11 de 2024, de Marsh McLennan: https://www.marsh.com/uy/es/services/cyber-risk/insights/how-to-strengthen-security-of-your-organization-with-red-team-tests.html

Watkins, J. (2023). *Exploring The Roles Of The Blue Team, The Red Team, And The Purple Team In Cybersecurity*. Recuperado el 29 de 11 de 2024, de Fusionauth: https://fusionauth.io/articles/security/blue-team-red-team-purple-team

Yasar, K. (2023). *Penetration testing*. Obtenido de TechTarget: https://www.techtarget.com/searchsecurity/definition/penetration-testing

ANEXO A. VIDEO DE PRESENTACIÓN DEL DESARROLLO DE LA ACTIVIDAD:

https://youtu.be/gCWwtBIhqZ0