José Carlos López Henestrosa

Incidentes de ciberseguridad

Tarea 3: Investigación de los incidentes de ciberseguridad

Índice

Fundamentos de la Plataforma de Defensa proactiva

Investiga en Internet cuáles son los fundamentos habituales de las plataformas de defensa profesionales, considerando distribuciones de Linux como sistema operativo base, plataformas de desarrollo colaborativo para proyectos de código abierto, y marcos de trabajo para desarrollo y aplicación de herramientas.

Los fundamentos habituales de las **plataformas de defensa profesionales en distribuciones Linux para el equipo azul** suelen compartir ciertos pilares, tales como el control de acceso obligatorio para reforzar la seguridad mediante la definición de políticas estrictas que controlan el acceso de procesos y usuarios a los recursos del sistema, y la implementación de cortafuegos y sistemas de detección de intrusos (IDS) para gestionar de forma eficiente el tráfico de red y la identificación de actividades sospechosas. Además, es esencial mantener el sistema y los paquetes instalados actualizados para obtener los parches de seguridad más recientes, así como usar protocolos seguros (HTTPS, SSH, FTPS, etc.) para cifrar los datos. Por último, es conveniente establecer políticas de seguridad rigurosas y estrictas para garantizar que solo el personal autorizado tenga acceso a recursos específicos y mitigar el riesgo de accesos no autorizados, junto con la deshabilitación del uso de cuentas por defecto como “Administrador”, “admin”, “root”, etc.

Además de todo lo mencionado anteriormente, para que el equipo azul implemente una defensa proactiva en distribuciones de Linux, es esencial contar con una plataforma integral que combine los siguientes fundamentos:

- **Gestión de la información y los eventos de seguridad (SIEM)**: Recopilar y analizar registros de eventos en tiempo real para detectar actividades sospechosas y generar alertas.
- **Sistemas de detección y respuesta en endpoints (EDR):** Monitorear dispositivos para identificar y responder a amenazas en tiempo real.
- **Sistemas de detección de intrusiones (IDS)**: Supervisar el tráfico de red para identificar actividades maliciosas o no autorizadas.
- **Honeypots**: Sistemas señuelo diseñados para atraer y detectar actividades maliciosas, permitiendo el estudio de tácticas empleadas por atacantes.
- **Respuesta a incidentes**: Facilitar la gestión y coordinación durante y después de un incidente de seguridad.
- **Análisis forense y sandboxing**: Permitir el análisis detallado de archivos sospechosos y comportamientos maliciosos en entornos controlados.

Dentro del marco de distribuciones Linux, podemos usar **Wazuh**, una plataforma de código abierto que combina todos los fundamentos mencionados anteriormente. Además, ofrece detección de intrusiones basada en host (HIDS), análisis de seguridad y cumplimiento mediante auditorías de configuración y evaluación de vulnerabilidades, monitorización de infraestructura e integración con Elastic Stack, lo que permite tener una visualización avanzada de datos y análisis en tiempo real mediante *dashboards* personalizables.

Respecto a las **plataformas de desarrollo colaborativo para proyectos de código abierto**, podemos destacar características comunes entre ellas, como el control de versiones, que permite llevar un registro detallado de los cambios en el código y facilita la colaboración y la reversión a estados anteriores si es necesario. Además, esto posibilita centralizar el código en un único repositorio, lo cual permite a los colaboradores clonar y modificar el código de manera organizada. A su vez, estas plataformas cuentan con herramientas de comunicación, como foros y seguimiento de incidencias, para mantener una comunicación fluida con el fin de resolver problemas de forma conjunta. Como aliciente, la integración continua (CI) permite automatizar pruebas y despliegues, lo cual asegura que las nuevas contribuciones no introduzcan errores y que el software se mantenga en un estado funcional.

Dentro de las plataformas de desarrollo colaborativo destacadas se encuentra **GitHub**, una de las más populares. También existen otras como GitLab y Bitbucket. Todas ellas tienen en común el soporte de Git, la herramienta de control de versiones más extendida, y las características comentadas en el párrafo anterior.

En relación con los **marcos de trabajo, o *frameworks***, es importante apuntillar que son estructuras predefinidas que proporcionan un conjunto de herramientas, librerías y convenciones diseñadas para simplificar y optimizar el proceso de desarrollo de software. Al estandarizar la arquitectura, los desarrolladores pueden centrarse en la lógica específica de sus aplicaciones, lo que reduce el tiempo dedicado a tareas repetitivas y, en definitiva, mejora la eficiencia general del desarrollo.

En el ámbito de la ciberseguridad, **MITRE ATT&CK** es un marco ampliamente utilizado para describir tácticas, técnicas y procedimientos (TTPs) utilizados por actores de amenazas. Para consultarlo y aprovecharlo eficazmente, existen varios marcos de trabajo y metodologías que pueden utilizarse para el equipo azul, tales como los siguientes:

- **Simulaciones de ataques avanzados**: Implementar ejercicios de *red teaming* donde se simulan ataques basados en las técnicas documentadas en MITRE ATT&CK. Esto permite al equipo azul identificar vulnerabilidades y evaluar la eficacia de sus defensas en un entorno controlado.
- **Caza de amenazas (*threat hunting*)**: Utilizar el marco para desarrollar hipótesis de posibles actividades maliciosas dentro de la red. Al mapear comportamientos sospechosos con las técnicas de MITRE ATT&CK, los analistas pueden detectar y neutralizar amenazas que podrían pasar desapercibidas por soluciones de seguridad tradicionales.
- **Evaluación y fortalecimiento de controles de seguridad**: Comparar las técnicas descritas en MITRE ATT&CK con las capacidades actuales de detección y respuesta de la organización.

Esto ayuda a identificar brechas en la cobertura de seguridad y priorizar la implementación de controles adicionales o mejoras en los existentes.

- **Desarrollo de casos de uso para SIEM**: Crear reglas y alertas en las plataformas de Gestión de Información y Eventos de Seguridad (SIEM) basadas en las técnicas de MITRE ATT&CK. Esto mejora la capacidad de detección temprana y respuesta ante incidentes específicos.
- **Formación y concienciación**: Capacitar al personal de seguridad en las tácticas y técnicas descritas en MITRE ATT&CK. Un equipo bien informado puede reconocer y responder más eficazmente a las actividades maliciosas.
- **Evaluación continua de riesgos**: Utilizar MITRE ATT&CK para mantenerse actualizado sobre las técnicas que los ciberdelincuentes emplean para adaptar las estrategias de defensa en consecuencia.

Herramientas de defensa proactiva para Equipo Azul

Busca en Internet información sobre las herramientas que se utilizan habitualmente en las configuraciones de los Equipos Azules, basándote en los Fundamentos de las Plataformas de Defensa identificados en el apartado anterior. Una vez las identifiques, selecciona un conjunto adecuado de dichas herramientas, indica sus funciones y recomiéndalas como aplicaciones base para la plataforma de defensa proactiva del Equipo Azul.

Antes de entrar en más detalle sobre las herramientas, es importante señalar que los equipos azules en el ámbito de la ciberseguridad son responsables de la defensa activa de los sistemas de información, enfocándose en la protección, monitoreo y respuesta ante incidentes de seguridad. Para llevar a cabo estas tareas de manera activa, emplean una variedad de herramientas especializadas, entre las que se encuentran las siguientes:

- **Herramientas de gestión de la información y los eventos de seguridad (SIEM)**
  - **Splunk Enterprise Security**: Ofrece análisis avanzados y monitoreo en tiempo real para detectar y responder a amenazas.
  - **IBM QRadar**: Proporciona análisis de seguridad inteligentes para identificar y priorizar incidentes en toda la organización.
  - **LogRhythm NextGen SIEM**: Combina monitoreo de seguridad, análisis forense y respuesta a incidentes en una única plataforma.
  - **ArcSight Enterprise Security Manager (ESM)**: Plataforma de análisis de seguridad que ayuda a identificar y mitigar amenazas en tiempo real.
  - **AlienVault Unified Security Management (USM)**: Integra capacidades de SIEM con gestión de vulnerabilidades y detección de intrusiones.
  - **Graylog**: Herramienta de gestión de logs que facilita el análisis y la visualización de datos para la detección de amenazas.
  - **SolarWinds Security Event Manager**: Ofrece correlación de eventos de seguridad y respuesta automatizada a incidentes.
  - **McAfee Enterprise Security Manager**: Proporciona monitoreo de seguridad en tiempo real y gestión de riesgos.

- **Securonix**: Plataforma SIEM basada en la nube que utiliza análisis avanzados para detectar amenazas.
- **Exabeam Fusion SIEM**: Combina SIEM y XDR para ofrecer detección y respuesta ante amenazas de manera eficiente.

- **Sistemas de detección y respuesta en endpoints (EDR)**
  - **SentinelOne Singularity Endpoint**: Plataforma que unifica datos y flujos de trabajo para ofrecer visibilidad y control sobre los endpoints.
  - **CrowdStrike Falcon**: Proporciona protección en tiempo real contra amenazas mediante inteligencia artificial y aprendizaje automático.
  - **Microsoft Defender for Endpoint**: Solución de EDR que integra protección avanzada contra amenazas y capacidades de respuesta automatizada.
  - **Trend Micro Apex One**: Ofrece detección y respuesta automatizada ante amenazas, junto con análisis de comportamiento.
  - **Symantec Endpoint Detection and Response**: Proporciona monitoreo continuo y análisis avanzado para identificar y mitigar amenazas en endpoints.
  - **Carbon Black Endpoint**: Plataforma que ofrece protección avanzada mediante análisis de comportamiento y monitoreo continuo.
  - **Kaspersky Endpoint Detection and Response**: Combina análisis de causa raíz con respuesta automatizada a incidentes.
  - **Cynet 360**: Plataforma integral que incluye EDR, NGAV y análisis de comportamiento para una protección completa.
  - **Check Point Harmony Endpoint**: Solución que integra EDR, EPP y XDR para ofrecer una protección unificada.
  - **Sophos Intercept X**: Combina capacidades de EDR con inteligencia artificial para detectar y responder a amenazas avanzadas.

- **Sistemas de detección de intrusiones (IDS)**
  - **Snort**: Sistema de prevención y detección de intrusiones de código abierto ampliamente utilizado.
  - **Suricata**: Motor de detección de amenazas de alto rendimiento que ofrece análisis de tráfico en tiempo real.
  - **Zeek (anteriormente Bro)**: Plataforma de monitoreo de red que proporciona análisis detallado del tráfico para detectar actividades sospechosas.
  - **OSSEC**: Sistema de detección de intrusiones basado en host que monitorea logs y archivos en busca de anomalías.
  - **Security Onion**: Distribución Linux que integra múltiples herramientas de seguridad para la detección y análisis de intrusiones.
  - **Prelude SIEM**: Framework híbrido de detección de intrusiones que combina análisis de eventos y correlación de logs.

- **Sagan**: Motor de correlación de logs en tiempo real que complementa sistemas IDS para una detección más precisa.
- **AIDE (Advanced Intrusion Detection Environment)**: Herramienta que verifica la integridad de archivos y directorios para detectar modificaciones no autorizadas.
- **OpenWIPS-NG**: Sistema de prevención de intrusiones inalámbricas diseñado para detectar y mitigar amenazas en redes Wi-Fi.
- **Fail2Ban**: Programa que protege servidores contra ataques de fuerza bruta mediante la monitorización de logs y el bloqueo de direcciones IP sospechosas.

- **Honeypots**
  - **Kippo**: Honeypot diseñado para simular un servidor SSH vulnerable y registrar intentos de intrusión.
  - **Cowrie**: Fork de Kippo que añade funcionalidades adicionales para emular entornos SSH y Telnet.
  - **Dionaea**: Honeypot que pretende capturar malware explotando vulnerabilidades en servicios de red.
  - **Glastopf**: Honeypot de aplicaciones web que emula vulnerabilidades para atraer y registrar ataques dirigidos a sitios web.
  - **Honeyd**: Herramienta que permite crear hosts virtuales en una red para simular sistemas operativos y servicios diversos.
  - **Conpot**: Honeypot diseñado para emular dispositivos de sistemas de control industrial (ICS) y atraer ataques dirigidos a infraestructuras críticas.
  - **Amun**: Honeypot de código abierto que captura y analiza malware en entornos controlados.
  - **T-Pot**: Plataforma que integra múltiples honeypots y herramientas de análisis para proporcionar una solución completa de detección de amenazas.
  - **Honeytrap**: Framework flexible que permite la implementación de honeypots personalizados, facilitando la captura y análisis de diversas amenazas en entornos controlados.
  - **Artillery:** Además de funcionar como un honeypot, esta herramienta ofrece capacidades de monitoreo y alerta, permitiendo configurar puertos comunes para detectar y registrar actividades sospechosas.

- **Herramientas de respuesta a incidentes**
  - **AlienVault USM**: Plataforma integral que combina la detección de amenazas, respuesta a incidentes y gestión de cumplimiento, proporcionando supervisión y reparación de seguridad para entornos locales y en la nube.
  - **CrowdStrike Falcon**: Solución basada en la nube que ofrece protección avanzada contra amenazas, combinando prevención de malware, detección de comportamiento y respuesta a incidentes en tiempo real.
  - **Cortex XSOAR**: Plataforma de orquestación, automatización y respuesta de seguridad

(SOAR) que integra diversas herramientas y facilita la gestión eficiente de incidentes mediante playbooks automatizados.

- **TheHive**: Aplicación de código abierto diseñada para gestionar y coordinar respuestas a incidentes de seguridad, permitiendo la colaboración entre equipos y el seguimiento detallado de casos.
- **MISP (Malware Information Sharing Platform)**: Herramienta de código abierto que facilita el intercambio de información sobre amenazas y la colaboración entre organizaciones para mejorar la respuesta a incidentes.
- **RTIR (Request Tracker for Incident Response)**: Sistema de gestión de tickets especializado en la respuesta a incidentes de seguridad, ayudando a organizar y priorizar tareas dentro del equipo.
- **GRR Rapid Response**: Framework de respuesta a incidentes desarrollado por Google, enfocado en la investigación y monitoreo de sistemas a gran escala.
- **Carbon Black Response**: Proporciona visibilidad continua y análisis en tiempo real de actividades en endpoints, facilitando la detección y respuesta rápida a amenazas avanzadas.
- **SANS Investigative Forensic Toolkit (SIFT)**: Conjunto de herramientas forenses digitales que permite a los profesionales realizar investigaciones exhaustivas y responder eficazmente a incidentes de seguridad.
- **Security Onion**: Distribución Linux de código abierto para monitoreo, detección y respuesta a intrusiones, integrando múltiples herramientas de seguridad en una plataforma unificada.

- **Herramientas de análisis forense y sandboxing**
  - **EnCase Forensic**: Software de análisis forense digital que permite la recopilación, preservación y análisis de evidencia de manera eficiente y conforme a estándares legales.
  - **Autopsy**: Interfaz gráfica para The Sleuth Kit que facilita el análisis forense de discos y la recuperación de datos, ampliamente utilizada en investigaciones digitales.
  - **FTK (Forensic Toolkit)**: Herramienta de AccessData que ofrece capacidades avanzadas para el análisis forense de sistemas, incluyendo recuperación de archivos eliminados y análisis de registros.
  - **Wireshark**: Analizador de protocolos de red que permite capturar y examinar el tráfico en tiempo real, siendo esencial para el análisis forense de redes.
  - **Cuckoo Sandbox**: Sistema de análisis de malware de código abierto que automatiza la ejecución y observación de archivos sospechosos en entornos aislados para detectar comportamientos maliciosos.
  - **VirtualBox**: Herramienta de virtualización de código abierto que permite desplegar máquinas virtuales para realizar pruebas y análisis en entornos controlados sin afectar al sistema anfitrión.
  - **VMware Workstation**: Plataforma de virtualización que facilita la creación y gestión de máquinas virtuales, utilizada comúnmente en análisis forense y pruebas de seguridad.

- **Xplico**: Herramienta de análisis forense de redes que reconstruye los contenidos de las capturas de tráfico, como correos electrónicos, navegación web y otros protocolos.
- **Bulk Extractor**: Programa que analiza imágenes de disco y archivos para extraer información relevante, como correos electrónicos, números de tarjetas de crédito y otros datos sensibles.
- **Bitdefender Sandbox Analyzer**: Herramienta que utiliza modelos de heurística del comportamiento y aprendizaje automático para analizar archivos sospechosos en un entorno aislado, mejorando la detección de amenazas avanzadas.

Bibliografía

- WeLiveSecurity. (2021, 26 de marzo). *Defensa en profundidad: cómo implementar esta estrategia de ciberseguridad*. https://www.welivesecurity.com/la-es/2021/03/26/defensa-profundidad-que-es-como-implementar-estrategia-ciberseguridad
- Remove Group. (2024, 11 de julio). *¿Qué es la ciberseguridad proactiva?* https://www.removegroup.com/que-es-la-ciberseguridad-proactiva/
- Global Owls. *La importancia de los feeds de inteligencia sobre amenazas en la ciberdefensa moderna.* https://globalowls.com/es/importance-threat-intelligence-feeds-modern-cyber-defense
- MTechnology. (2023, 7 de marzo). *¿Qué son las plataformas de desarrollo de software y para qué sirven?* https://mtechnology.pro/blog/que-son-las-plataformas-de-desarrollo-de-software-y-para-que-sirven
- Wikipedia. (2024, 3 de diciembre). *Framework.* https://es.wikipedia.org/wiki/Framework
- VGST. (2022, 24 de marzo). *Frameworks de Ciberseguridad: Modelos y Estándares.* https://vgst.net/blog/cloud/frameworks-de-ciberseguridad-principales-modelos-y-estandares
- Palo Alto Networks. *¿Qué es el marco MITRE ATT&CK?* https://www.paloaltonetworks.es/cyberpedia/what-is-mitre-attack-framework
- Tu Consultor TI. *MITRE ATT&CK: Un Marco Esencial para la Defensa Cibernética.* https://www.tuconsultorti.com/ciberseguridad/mitre-attack/
- Cyrebro. *Fortalezca su postura de seguridad con el framework MITRE ATT&CK*. https://www.cyrebro.io/es/blog/fortalezca-su-postura-de-seguridad-con-el-framework-mitre-attck
- Delta Project. (2025, 17 de enero). *Blue team en ciberseguridad: definición, funciones y herramientas*. https://www.deltaprotect.com/blog/blue-team-ciberseguridad
- S2 Grupo. (2024, 13 de marzo). *Blue team de ciberseguridad: qué es y qué funciones cumple*. https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/
- Ciberseguridad. *Las mejores herramientas del equipo azul*. https://ciberseguridad.com/herramientas/equipo-azul/
- Research AIMultiple. (2025, 20 de febrero) *Top 10+ SIEM Systems: How to Choose the Best Solution.* https://research.aimultiple.com/siem-tools/
- Geeks for Geeks. (2025, 7 de enero). *Top 10 SIEM Tools in 2025.* https://www.geeksforgeeks.org/top-siem-tools/
- Atera. (2025, 30 de enero). *Top EDR tools for MSPs & IT teams to enhance cybersecurity.* https://www.atera.com/blog/best-edr-tools/
- Informática Forense. *Las 9 mejores herramientas de respuesta a incidentes de seguridad para pequeñas y medianas empresas.*

https://www.informaticaforense.com.co/las-9-mejores-herramientas-de-respuesta-a-incidentes-de-seguridad-para-pequenas-y-empresas

- KeepCoding. (2024, 27 de junio). *5 herramientas de sandboxing.* https://keepcoding.io/blog/herramientas-de-sandboxing
- GeekFlare. (2024, 14 de mayo). *22 herramientas GRATUITAS de investigación forense para expertos en seguridad informática*. https://geekflare.com/es/forensic-investigation-tools/
- InvGate. (2024, 5 de febrero). *Los 11 mejores software de Gestión de Incidentes de 2025.* https://blog.invgate.com/es/software-de-gestion-de-incidencias