HERRAMIENTAS DE SOFTWARE LIBRE PARA CIBERSEGURIDAD

M.Sc. ING. RICARDO NARANJO FACCINI

gerencia@skinait.com

Ingeniería Civil

Universidad de los Andes

Bogotá, Colombia

RESUMEN

Se proporciona una visión general de diversas herramientas de software libre aplicables a la ciberseguridad, organizadas en cinco categorías funcionales: ***Preparativas:*** *Estas herramientas están diseñadas para facilitar la planificación y la preparación de medidas de seguridad. Incluyen herramientas para llevar el inventario de activos o para redactar las políticas y el SGSI;* ***Preventivas:*** *Estas herramientas se utilizan para evitar que ocurran incidentes de seguridad. Incluyen software para el análisis de vulnerabilidades, gestión de configuraciones y control de accesos, que ayudan a prevenir ataques y errores antes de que ocurran;* ***Detectivas:*** *Las herramientas en esta categoría están enfocadas en la identificación de problemas y anomalías en tiempo real. Incluyen sistemas de monitoreo y detección de intrusiones que permiten a los equipos de seguridad identificar amenazas y actividades sospechosas de manera proactiva;* ***Reactivas:*** *Estas herramientas se emplean para responder a incidentes de seguridad una vez que han ocurrido. Incluyen plataformas para el*

análisis forense y la gestión de incidentes, que permiten investigar y mitigar los efectos de los ataques; ***Retrospectivas:*** *Aunque no se identificaron herramientas específicas de software libre para actividades retrospectivas, las funciones correspondientes se encuentran integradas en las herramientas de las categorías anteriores. Estas herramientas permiten realizar evaluaciones y análisis post-incidente para mejorar la seguridad a largo plazo.*

El artículo destaca cómo estas herramientas, al ser utilizadas en conjunto, proporcionan una cobertura integral para la gestión de la seguridad en diferentes fases del ciclo de vida de los incidentes.

Es importante destacar que, si bien el hecho de que un software esté protegido por una licencia de software libre no garantiza su calidad o seguridad, es necesario revisar la actividad de la comunidad que rodea a la herramienta, como la generación de tutoriales en diversos idiomas y la frecuente generación de nuevas versiones con correcciones de errores y nuevas funcionalidades, como una medida de garantía de calidad y seguridad.

1. INTRODUCCIÓN

La popularidad del software libre ha crecido significativamente en los últimos años, ya que cada vez más personas y organizaciones reconocen las ventajas de utilizar software de código abierto en lugar de software privativo. Una de las áreas donde el software libre ha ganado terreno es en la ciberseguridad, ya que existen numerosas herramientas de seguridad de código abierto disponibles que son utilizadas por profesionales de la seguridad en todo el mundo.

Sin embargo, es importante destacar que el hecho de que un software esté protegido por una licencia de código abierto no es garantía de calidad ni de seguridad. Lo mismo sucede con el software privativo. Aunque el código abierto permite que cualquiera pueda ver el código fuente y modificarlo, esto no significa que el software sea seguro o esté libre de errores. De hecho, algunos proyectos de software libre y privativo pueden contener errores o vulnerabilidades que pueden ser explotados por atacantes malintencionados.

Entonces, ¿cómo podemos estar seguros de que el software de seguridad que estamos utilizando es seguro y confiable? La respuesta radica en la comunidad que rodea al proyecto. Cuando se trata de software, la comunidad de desarrolladores y usuarios es crucial para garantizar la calidad y seguridad del software.

Una comunidad activa y comprometida en torno a un proyecto de software es una buena señal de que el software es seguro y confiable. Una comunidad activa significa que hay muchos desarrolladores y usuarios trabajando en el proyecto, discutiendo los problemas y soluciones, y compartiendo información sobre el software.

Además, una comunidad activa también significa que hay muchas conversaciones en línea, tutoriales y documentación disponible en varios idiomas, lo que facilita el aprendizaje y la utilización del software. Otro indicador de calidad y seguridad del software es la frecuencia con la que se publican nuevas versiones y actualizaciones. Los proyectos de software con una comunidad activa suelen publicar nuevas versiones con frecuencia, lo que indica que están corrigiendo errores y añadiendo nuevas funcionalidades de forma constante. La publicación frecuente de nuevas versiones es un buen indicador de que el software está siendo mantenido y actualizado activamente.

2. DESARROLLO

Clasificación del software libre para ciberseguridad

El software libre para ciberseguridad tiene diversas aplicaciones y se clasifica de acuerdo con el tipo de actividad de ciberseguridad que atiende, las cuales pueden ser: Preparativas, Preventivas, Detectivas, Reactivas o Retrospectivas. Cabe aclarar que algunas herramientas de software libre pueden atender a varias de éstas actividades.

Para actividades Preparativas

a) Acceso remoto

- **ssh:** secure shell, es un comando utilizado para conectarse a un servidor remoto de forma segura utilizando el protocolo SSH. Al ejecutar el comando ssh, se puede ingresar la dirección IP o el nombre de dominio del servidor y establecer una sesión de terminal remota segura.

- **gsh:** el group shell es similar al ssh, con la diferencia que los comandos que se ingresan en el computador maestro queda inmediatamente replicado en los otros computadores.

- **Xwindows:** El entorno gráfico de UNIX/Linux es de resaltar, dado que desde su creación en los años 60 fue pensado como un entorno de red y el despliegue remoto de aplicativos siempre ha estado presente en éste tipo de entornos, tanto para desplegar aplicativos en ventanas individuales como para todo el escritorio. Se puede utilizar para entornos de programación y despliegue remoto, facilitando la administración y ejecución de herramientas de ciberseguridad en máquinas remotas a través de interfaces gráficas, sin necesidad de acceso físico.

b) Documentación del SGSI

- **LibreOffice y OpenOffice:** La suite de oficina de UNIX/Linux es tan poderosa como las diferentes versiones de ellas en el mundo privativo, se encontrarán algunas funcionalidades más poderosas o menos que en el mundo privado, al igual que se destacarán funcionalidades novedosas como el graficador de ecuaciones matemáticas y algunas funcionalidades que se consiguen en el mundo

privado harán falta en éstas dos suites. Sin embargo, a nivel general pueden equipararse a las más famosas.

c) Automatización

- **crontab:** es un comando utilizado para programar tareas y comandos para que se ejecuten en momentos específicos, utilizando el cron daemon. Al ejecutar el comando crontab, se puede editar el archivo de configuración cron del usuario y programar tareas para que se ejecuten en diferentes momentos y frecuencias.

d) Protección de contraseñas

La protección de contraseñas es una herramienta que puede proteger los datos personales y de inicio de sesión almacenados en un ordenador. Puede almacenar contraseñas de forma segura y generar contraseñas fuertes para una mayor seguridad.

- **KeePass:** Es un administrador de contraseñas de código abierto y gratuito que se utiliza para almacenar y gestionar contraseñas encriptadas en una base de datos segura. KeePass ofrece una forma fácil y segura de almacenar todas las contraseñas y credenciales importantes en un solo lugar. La base de datos de KeePass está protegida por una contraseña maestra y puede ser encriptada con varios algoritmos de cifrado para proporcionar un nivel adicional de seguridad.

e) Gestión de activos

- **GLPI:** es una herramienta de gestión de activos de TI y de mesa de ayuda de código abierto. Se utiliza para gestionar la información y los problemas relacionados con los recursos de TI, incluyendo la gestión de inventario, la gestión de incidentes y la gestión de cambios. GLPI también puede utilizarse para realizar seguimiento y resolver problemas de seguridad.

Para actividades Preventivas

a) Inteligencia

- **MISP (Malware Information Sharing Platform):** es una plataforma de compartición de información sobre amenazas. Permite compartir información sobre amenazas de forma segura entre organizaciones para mejorar la detección y respuesta a amenazas.

  Es una plataforma de software libre para compartir, almacenar y correlacionar indicadores de compromiso (IoC) y otros datos de inteligencia de amenazas cibernéticas. MISP permite a las organizaciones colaborar y mejorar su defensa mediante la inteligencia de amenazas compartida.

- **Maltego:** Una poderosa herramienta de OSINT (Open Source Intelligence) que permite la visualización de relaciones y conexiones entre entidades. En ciberseguridad, se utiliza para investigaciones de inteligencia, mapeando redes sociales, dominios, correos electrónicos, y más, para descubrir vínculos que puedan revelar amenazas o actores maliciosos.

- **T-Pot:** Es un honeypot de código abierto listo para usar que está diseñado para atraer y analizar las actividades de ciberdelincuentes. T-Pot permite a los equipos de ciberseguridad monitorear ataques en tiempo real y recopilar información valiosa sobre técnicas y tácticas utilizadas por los atacantes.

b) Criptografía

- **Criptografía en una dirección:** El comando md5sum se utiliza para calcular el hash MD5 de un archivo, lo que permite verificar la integridad de su contenido. Por ejemplo, "md5sum archivo.txt" generaría el hash MD5 del archivo.txt. sha256sum es un comando utilizado para calcular el valor hash de un archivo utilizando el algoritmo SHA-256. Al ejecutar el comando sha256sum, se puede calcular el hash de un archivo y verificar su integridad, ya que cualquier cambio en el archivo cambiará su hash.

- **Criptografía simétrica:** El comando openssl permite cifrar y descifrar archivos utilizando algoritmos de cifrado simétrico como AES o DES. Por ejemplo, "openssl enc -aes256 -in archivo.txt -out archivo.cifrado" cifrar el archivo.txt con AES-256 y generar el archivo cifrado archivo.cifrado.

- **Criptografía asimétrica:** El comando openssl también se puede utilizar para generar claves y certificados digitales para la criptografía asimétrica. Por ejemplo, "openssl genpkey -algorithm RSA -out clave.privada" generaría una clave privada RSA y "openssl req -new -key clave.privada -out certificado.csr" generaría una solicitud de certificado digital que se puede enviar a una autoridad de certificación para obtener un certificado digital que se puede utilizar para cifrar y descifrar datos utilizando la clave pública correspondiente a la clave privada generada.

c) Backups

- **rsync:** Es un comando utilizado para sincronizar archivos y directorios entre sistemas, de forma segura y eficiente. Al ejecutar el comando rsync, se pueden sincronizar archivos y directorios entre sistemas utilizando diferentes protocolos de transferencia de archivos, como SSH. Es valioso para replicar datos de manera segura y eficiente entre diferentes sistemas o para crear respaldos en tiempo real.

- **grsync:** Es una interfaz gráfica para rsync, que facilita la configuración y el uso de rsync para usuarios que prefieren trabajar en un entorno visual. Es útil en la gestión de sincronización y backups seguros en sistemas de ciberseguridad.

- **borg:** Es una herramienta de respaldo (backup) que se especializa en crear copias de seguridad eficientes, seguras y comprimidas. En ciberseguridad, Borg es útil para asegurar datos críticos y garantizar la continuidad de la operación en caso de incidentes de seguridad.

- **pikabackup:** Es una interfaz gráfica para Borg, facilitando a los usuarios menos experimentados la creación y gestión de copias de seguridad sin necesidad de utilizar la línea de comandos. Es útil para realizar backups en entornos donde la ciberseguridad es prioritaria.

d) Antimalware

Un antivirus es una herramienta que protege un sistema contra malware y virus. Puede escanear archivos y programas para detectar y eliminar cualquier amenaza.

- **ClamAV:** Es una herramienta de seguridad de código abierto utilizada para detectar y eliminar virus, troyanos, malware y otras amenazas en sistemas Unix y Windows. ClamAV es una herramienta gratuita y multiplataforma que utiliza una base de datos actualizada de firmas de virus para escanear archivos y directorios en busca de amenazas. ClamAV también se puede integrar en sistemas de correo electrónico y escanear el tráfico entrante y saliente para detectar correos electrónicos con archivos adjuntos maliciosos previniendo que lleguen a los sistemas Windows que puedan ser afectados por el malware entrante.

- **Pdf-parser.py:** es un script de Python que se utiliza para analizar archivos PDF y extraer información de ellos. Este script es de código abierto y se puede descargar de forma gratuita desde su sitio web. Pdf-parser.py puede ser utilizado para extraer objetos PDF como fuentes, imágenes, scripts, y para analizar la estructura interna de un archivo PDF. También puede utilizarse para decodificar objetos codificados en Base64 y FlateDecode, lo que puede ser útil para analizar archivos maliciosos.

- **Pdftools:** es otra herramienta de software libre para analizar archivos PDF. Esta herramienta está diseñada para escanear archivos PDF en busca de virus y malware. Además, pdftools puede ser utilizado para extraer información de los archivos PDF, incluyendo metadatos, fuentes, scripts, y objetos embebidos.

- **RKhunter:** Es una herramienta de seguridad que busca detectar malware, rootkits y otras posibles amenazas en sistemas Linux y Unix. La herramienta realiza comprobaciones en los archivos del sistema, las bibliotecas compartidas y los binarios, para detectar cualquier alteración inesperada. También verifica los servicios activos y los puertos abiertos en busca de posibles vulnerabilidades.

e) Capacitación y sensibilización

- **Moodle:** Es una plataforma de aprendizaje en línea de código abierto. En ciberseguridad, Moodle se utiliza para capacitar y sensibilizar al personal en temas de seguridad, proporcionando un entorno estructurado para cursos, talleres y materiales educativos sobre ciberseguridad.

- **Jitsi Meet:** Es una solución de videoconferencia de código abierto que garantiza la privacidad y seguridad en las comunicaciones. Es ideal para reuniones internas, capacitaciones y cualquier otra interacción remota en entornos donde la seguridad es crítica.

- **OBS (Open Broadcaster Software):** Es una herramienta de código abierto para la grabación de video y transmisión en vivo. En ciberseguridad, OBS puede utilizarse para crear videotutoriales, webinars, y otras formas de contenido educativo o de sensibilización en seguridad informática.

- **Pitivi y OpenShot:** Son editores de vídeo de código abierto. En ciberseguridad, estas herramientas son útiles para editar videos educativos, tutoriales, o registros visuales de eventos de capacitación, brindando una forma efectiva de compartir conocimiento en seguridad.

f) Detección de vulnerabilidades

- **Nessus:** identificador de vulnerabilidades que permite escanear sistemas y aplicaciones en busca de vulnerabilidades conocidas y desconocidas.

- **Nikto:** Escáner de vulnerabilidades de servidores web por medio de línea de comandos, busca en particular archivos/CGI peligrosos, software de servidor obsoleto y otros problemas.
- **Lynis:** es una herramienta de auditoría de seguridad que escanea sistemas UNIX y Linux en busca de vulnerabilidades. Proporciona informes detallados sobre la configuración del sistema, la seguridad y las posibles vulnerabilidades.

- **OpenVAS (Open Vulnerability Assessment System):** Es un marco de software libre para escaneo y gestión de vulnerabilidades. En ciberseguridad, OpenVAS permite identificar y evaluar posibles vulnerabilidades en los sistemas, ayudando a las organizaciones a fortalecer su postura de seguridad.

- **AlienVault OSSIM:** Es una plataforma unificada de gestión de eventos e información de seguridad (SIEM) de código abierto. En ciberseguridad, AlienVault permite la correlación de eventos de seguridad, detección de amenazas y gestión de incidentes, integrando múltiples herramientas de seguridad en un solo panel.

g) Pruebas de penetración

- **Metasploit:** Es una plataforma de pruebas de penetración (pentesting) ampliamente utilizada que permite a los profesionales de la seguridad realizar ataques simulados para identificar vulnerabilidades en sistemas informáticos. Metasploit ofrece una vasta base de datos de exploits, payloads y herramientas auxiliares que permiten realizar pruebas de penetración completas, desde la explotación de vulnerabilidades hasta la post-explotación y el análisis de la seguridad de los sistemas.

- **Armitage:** Es una interfaz gráfica para Metasploit que facilita la ejecución de pruebas de penetración y ciberataques simulados. Armitage permite la automatización de muchas tareas complejas, como la selección de exploits y payloads, y proporciona una vista gráfica de los objetivos comprometidos. Es ideal para quienes prefieren un entorno visual para gestionar sus pruebas de seguridad, especialmente en entornos colaborativos.

- **Kali Linux:** Es una distribución de Linux basada en Debian diseñada específicamente para pruebas de penetración y auditorías de seguridad. Incluye una vasta colección de herramientas preinstaladas para realizar pruebas de seguridad en redes, aplicaciones web, sistemas operativos y más. Kali Linux es la herramienta predilecta de los profesionales de la ciberseguridad para realizar análisis de vulnerabilidades, pruebas de penetración, y forense digital.

- **Cyborg Hawk Linux**: Es otra distribución de Linux orientada a la ciberseguridad, que al igual que Kali Linux, ofrece una amplia gama de herramientas para pruebas de penetración, análisis forense, y auditorías de seguridad. Cyborg Hawk se destaca por su enfoque en la seguridad ofensiva y defensiva, y su entorno personalizable, lo que la convierte en una opción potente para investigadores de seguridad y profesionales del pentesting.

- **Paladin Linux:** Es una distribución basada en Ubuntu diseñada para investigaciones forenses digitales. Incluye una colección de herramientas forenses para la recuperación de datos, análisis de discos, y la creación de imágenes forenses. Paladin Linux es ideal para investigadores que necesitan una solución portátil y completa para realizar análisis forense de dispositivos digitales y redes.

h) Control de red

- **Bind:** también conocido como Berkeley Internet Name Domain, es un servidor de nombres de dominio (DNS) de código abierto. Se utiliza para traducir nombres de dominio en direcciones IP y viceversa. Bind es compatible con muchos sistemas operativos, incluyendo Linux, Unix y Windows. Es una herramienta esencial para cualquier red que utilice DNS.

- **E2guardian:** Es un proxy web de código abierto que se utiliza para filtrar contenido en la red. Proporciona filtros de contenido para bloquear sitios web inapropiados o peligrosos, y es capaz de bloquear el acceso a contenido basado en palabras clave y categorías. E2guardian también puede utilizarse para monitorizar y registrar el tráfico de la red.

- **WireGuard:** es un protocolo de VPN de código abierto. Se utiliza para establecer conexiones VPN seguras entre dispositivos y redes. WireGuard utiliza criptografía de última generación para proteger las conexiones y es muy rápido y eficiente en términos de recursos. Además, WireGuard es fácil de configurar y utilizar.

- **Squid:** es un servidor proxy de código abierto que se utiliza para acelerar y optimizar el tráfico web. Squid se utiliza comúnmente para cachear contenido web y reducir la carga de los servidores web.

También puede utilizarse para filtrar y bloquear el acceso a sitios web no deseados. Squid es compatible con muchos sistemas operativos y es muy configurable.

- **Cortafuegos de escritorio:** Un cortafuegos de escritorio es una herramienta que controla el tráfico de red entrante y saliente en un ordenador individual. Puede bloquear el acceso no autorizado a un sistema y prevenir ataques externos.

- **iptables:** es un comando utilizado para configurar y administrar el firewall del sistema, incluyendo reglas de filtrado de paquetes y configuraciones de NAT. Al ejecutar el comando iptables, se pueden agregar, eliminar y modificar reglas del firewall y configuraciones de red.

- **Endian Firewall:** Es una distribución de seguridad basada en Linux que combina múltiples funciones de ciberseguridad en una sola solución, conocida como UTM (Unified Threat Management). Endian Firewall incluye firewall, VPN, antivirus, filtrado de contenido web, detección y prevención de intrusiones (IDS/IPS), y más. Es especialmente útil en pequeñas y medianas empresas que necesitan una solución todo en uno para proteger sus redes contra una variedad de amenazas sin necesidad de configurar y mantener múltiples herramientas separadas.

- **ModSecurity:** Es un firewall de aplicaciones web (WAF) de código abierto que proporciona protección contra una amplia gama de ataques web. Se integra con servidores web como Apache y Nginx, siendo esencial para proteger aplicaciones web contra inyecciones SQL, XSS, y otros ataques.

- **pfSense:** Es una distribución de firewall y enrutador basada en FreeBSD, ampliamente utilizada en entornos de ciberseguridad. pfSense ofrece características avanzadas de firewall, VPN (Red Privada Virtual), detección de intrusiones (a través de plugins como Snort), y filtrado de contenido, todo configurable a través de una interfaz web intuitiva. Es ideal para proteger redes corporativas, proporcionando una capa adicional de seguridad en el control del tráfico de red, segmentación de redes, y acceso remoto seguro.

Para actividades Detectivas

a) Auditoría de contraseñas

- **John the Ripper:** herramienta de cracking de contraseñas que permite probar diferentes combinaciones de contraseñas para romper la seguridad de cuentas de usuario. Se puede utilizar para auditar las contraseñas de los usuarios de una organización identificando quienes utilizan contraseñas débiles. Descifra contraseñas probando todas las combinaciones posibles o utilizando listas de palabras comunes mediante el manejo de una amplia gama de algoritmos de hash, incluidos MD5, SHA-1, SHA-256, entre otros.

- **Hydra:** Es una herramienta de prueba de penetración de redes que se utiliza para adivinar contraseñas. Permite probar miles de posibles contraseñas en un corto periodo de tiempo,

utilizando diferentes métodos, como el diccionario, la fuerza bruta y el ataque híbrido. Al igual que John the Ripper puede ser utilizada para auditar las contraseñas débiles que usen los usuarios de un sistema de información.

- **Hashcat:** Es una herramienta de cracking de contraseñas que utiliza la potencia de cálculo de la GPU para realizar ataques de fuerza bruta y ataques de diccionario contra contraseñas cifradas con algoritmos de hash. Está optimizado para aprovechar la potencia de cálculo de la GPU, lo que le permite realizar ataques de cracking de contraseñas a alta velocidad. Puede manejar una gran variedad de algoritmos de hash, incluidos MD5, SHA-1, SHA-256, bcrypt, entre otros

- **Aircrack-NG:** Es una suite de herramientas de seguridad inalámbrica que se utiliza para auditorías de redes Wi-Fi. Permite el monitoreo de redes, captura de paquetes, inyección de paquetes, y análisis de tráfico para descifrar claves WEP y WPA/WPA2. Se utiliza para auditar y evaluar la seguridad de redes Wi-Fi. Permite realizar ataques de descifrado de claves WEP y WPA/WPA2 utilizando técnicas como fuerza bruta, diccionario y ataques basados en la inyección de paquetes. Proporciona herramientas para monitoreo y captura de paquetes de red, así como para el análisis y descifrado de tráfico cifrado.

b) Monitoreo de recursos del equipo

Un monitor de procesos es una herramienta que rastrea todos los procesos que se ejecutan en un sistema y puede identificar cualquier proceso malicioso o sospechoso. Puede valorar la cantidad porcentual de CPU o de memoria RAM que están consumiendo.

Procesos y recursos

- **ps:** es un comando utilizado para mostrar información sobre los procesos en ejecución en el sistema. Al ejecutar el comando ps, se muestra una lista de procesos en ejecución, cada uno con su identificador de proceso (PID), estado, uso de recursos y otros detalles. Es útil para identificar procesos específicos y detener o matar procesos si es necesario.

- **Kill:** se utiliza para detener un proceso en ejecución enviando una señal a su identificador de proceso (PID). El usuario debe especificar el PID del proceso que desea detener y la señal que se enviará al proceso. La señal predeterminada es SIGTERM, que indica al proceso que se detenga de manera ordenada, pero también se pueden enviar otras señales, como SIGKILL, que fuerza al proceso a detenerse inmediatamente.

- **Killall:** se utiliza para detener todos los procesos que tengan el mismo nombre. En lugar de especificar el PID de un proceso, el usuario especifica el nombre del proceso. Killall envía la señal SIGTERM a todos los procesos con el nombre especificado.

- **nice:** Es un comando de Unix/Linux que permite ajustar la "prioridad de ejecución" de un proceso antes de que se inicie. En ciberseguridad, nice puede ser útil para gestionar los recursos del sistema durante pruebas intensivas, como escaneos de vulnerabilidades o análisis forense, asegurando que

  estas tareas no ralentice otros servicios críticos en el sistema. Al ajustar la prioridad con nice, los administradores pueden optimizar el rendimiento del sistema, dándole más o menos recursos a ciertos procesos según lo requiera la situación.

- **renice**: Es un comando similar a nice, pero se utiliza para cambiar la prioridad de un proceso que ya está en ejecución. En ciberseguridad, renice es útil cuando se necesita ajustar dinámicamente el uso de recursos del sistema, por ejemplo, si un escaneo de seguridad está consumiendo demasiados recursos y se requiere reducir su prioridad para mantener la estabilidad del sistema. renice permite a los administradores intervenir en tiempo real para gestionar la carga del sistema y asegurar que las operaciones críticas continúen funcionando sin interrupciones.

- **top:** Es una herramienta de línea de comandos en Unix/Linux que muestra en tiempo real los procesos que se están ejecutando en el sistema, ordenados por el uso de recursos como la CPU, la memoria, y el tiempo de ejecución. En ciberseguridad, top es útil para monitorear el sistema en busca de procesos sospechosos o maliciosos que puedan estar consumiendo recursos inusuales, lo que podría indicar un compromiso de seguridad. También permite a los administradores de sistemas identificar rápidamente cuellos de botella y ajustar prioridades con herramientas como nice y renice.

- **htop:** Es una versión mejorada y más interactiva de top que ofrece una interfaz más amigable y visual. htop permite a los usuarios visualizar los procesos en una estructura en árbol, facilitando la identificación de procesos secundarios y la relación entre procesos. En ciberseguridad, htop es útil para monitorear de forma más intuitiva el uso de recursos del sistema, permitiendo a los administradores detectar patrones anómalos o procesos que podrían estar vinculados a actividades maliciosas, como malware o minería de criptomonedas no autorizadas.

- **inxi:** Es una herramienta de línea de comandos que proporciona una detallada información sobre el sistema, incluyendo el hardware, la configuración de red, y los dispositivos conectados. En ciberseguridad, inxi es especialmente útil para realizar auditorías de seguridad y obtener un rápido resumen del estado del sistema. Puede ayudar a los administradores a verificar la integridad del hardware y las configuraciones, identificar dispositivos desconocidos o no autorizados, y asegurarse de que la infraestructura cumple con las políticas de seguridad establecidas.

- **Acct:** Es un conjunto de herramientas que registra la actividad del sistema y de los usuarios en sistemas Linux y Unix. Permite a los administradores de sistemas supervisar el uso de los recursos del sistema y detectar posibles problemas de rendimiento. Además, la herramienta puede utilizarse para generar informes de uso de recursos para facturación o fines de contabilidad.

- **which:** es un comando que permite encontrar la ubicación de un archivo ejecutable en el sistema. Esta herramienta puede ser útil para verificar la integridad de los archivos del sistema y detectar archivos maliciosos que se hayan instalado en el sistema.

- **Auditd:** es una herramienta de auditoría que registra eventos del sistema en sistemas Linux y Unix. Permite a los administradores de sistemas supervisar la actividad de los usuarios y detectar posibles intrusiones. La herramienta registra eventos de inicio de sesión, cambios en los archivos del sistema y otros eventos importantes.

- **Monitores de recursos:** Un monitor de recursos es una herramienta que se utiliza para medir y visualizar la utilización del hardware de un sistema informático, como la CPU, la memoria, el disco y la red. Proporciona información sobre el uso actual y el historial de uso, lo que permite al usuario realizar un seguimiento del rendimiento del sistema y detectar cualquier problema.

- **El monitor del sistema de mate y ksysguard:** son herramientas gráficas utilizadas para monitorear el sistema y visualizar información sobre el uso de recursos, los procesos en ejecución y otros detalles del sistema. Estas herramientas pueden ser útiles para identificar procesos que están consumiendo recursos excesivos o para monitorear el rendimiento del sistema en general.

- **Baobab:** Es una herramienta gráfica para analizar el espacio en disco. Proporciona información detallada sobre el tamaño de los archivos y carpetas, permitiendo identificar fácilmente los archivos más grandes y liberar espacio en disco.

- **Glances:** Es un monitor de sistema en línea de comandos que proporciona una visión general del uso del sistema en tiempo real. Permite supervisar la CPU, memoria, carga del sistema, uso de la red, entre otros.

Usuarios

- **who:** Es un comando que muestra información sobre los usuarios que están actualmente conectados al sistema, incluyendo su nombre de usuario, terminal y hora de inicio de sesión. Esta información puede ser útil para monitorear la actividad del sistema y detectar intentos de acceso no autorizado.

- **lastcomm:** Es una herramienta de software libre para sistemas Unix y Unix-like que proporciona información sobre los comandos que se han ejecutado recientemente en el sistema. Este programa lee los registros de contabilidad del sistema (también conocidos como registros de procesos), que registran información sobre los procesos que se ejecutan en el sistema, y muestra una lista de los comandos que se han ejecutado, junto con detalles como el usuario que los ejecutó, la hora y la duración de la ejecución.

Red

- **ip:** es un comando utilizado para configurar y mostrar información sobre la red y las interfaces de red en el sistema. Al ejecutar el comando ip, se pueden realizar tareas como configurar direcciones IP, agregar rutas y mostrar información detallada sobre las interfaces de red.

- **Tcpdump:** Tcpdump es una herramienta de línea de comandos que permite capturar y analizar el tráfico de red en tiempo real. Es una herramienta muy útil para la detección de problemas de red y para la investigación de ataques en la red. Tcpdump puede ser utilizado para capturar y analizar paquetes en la red en diferentes formatos,incluyendo el popular formato pcap utilizado por Wireshark y otras herramientas de análisis de tráfico de red.

  Tiene muchas opciones y filtros para personalizar la captura de paquetes, lo que permite a los usuarios capturar únicamente el tráfico que necesitan y evitar la sobrecarga de información innecesaria. Tcpdump puede filtrar el tráfico por dirección IP, puerto, protocolo, y muchas otras características.

  Además, Tcpdump tiene una capacidad limitada de decodificación de protocolos de red, lo que permite a los usuarios identificar los protocolos utilizados por los paquetes capturados. Tcpdump es una herramienta muy útil para la solución de problemas de red y la investigación de incidentes de seguridad.

- **netstat:** es un comando utilizado para mostrar información sobre la red y las conexiones de red activas. Al ejecutar el comando netstat, se muestra una lista de conexiones activas, incluyendo la dirección IP, el puerto y el estado de cada conexión. Es útil para identificar conexiones de red no deseadas o sospechosas y para monitorear la actividad de la red en general.

- **nslookup:** es un comando utilizado para realizar consultas de resolución de nombres de dominio (DNS) y obtener información sobre registros de recursos de DNS, como las direcciones IP asociadas a un nombre de dominio. Al ejecutar el comando nslookup, se puede ingresar un nombre de dominio y obtener la dirección IP correspondiente, o viceversa.

- **dig:** es similar a nslookup, pero proporciona información más detallada y opciones de configuración adicionales. Al ejecutar el comando dig, se pueden realizar consultas de DNS y obtener información detallada sobre los registros de recursos, incluyendo la dirección IP, la TTL y la autoridad del servidor.

- **whois:** es un comando que permite buscar información sobre un dominio o una dirección IP en bases de datos públicas. Esta herramienta puede ser útil para obtener información sobre un sitio web o identificar el propietario de una dirección IP que se está utilizando para realizar actividades maliciosas.

- **traceroute:** es una herramienta que permite seguir la ruta que sigue un paquete de datos desde un origen hasta un destino. Esto puede ser útil para diagnosticar problemas de red y detectar posibles puntos de fallo o de ataque en la comunicación.

c) Monitoreo de equipos en una red

- **Nmap:** Es una herramienta de escaneo de red de código abierto que se utiliza para descubrir hosts y servicios en una red. Nmap puede utilizarse para encontrar vulnerabilidades y puertos abiertos en una red, y también se puede utilizar para identificar sistemas operativos y servicios en la red. Nmap es una herramienta esencial para cualquier profesional de la seguridad de la red.

- **Wireshark:** Es un analizador de protocolos de red de código abierto. Se utiliza para capturar y analizar el tráfico de red en tiempo real. Wireshark puede utilizarse para detectar problemas de seguridad y de red, y también puede utilizarse para examinar la comunicación entre aplicaciones. Wireshark es una herramienta muy versátil y es una de las más utilizadas en la industria.

- **OSQuery:** sistema de monitorización y gestión de sistemas que permite obtener información detallada sobre los sistemas en tiempo real, como el estado de los procesos, el uso de la memoria y la red, y otros aspectos de la configuración.

- **aide:** Es una herramienta de detección de intrusiones similar a tripwire que permite verificar la integridad de los archivos del sistema en busca de cambios no autorizados. AIDE puede generar una base de datos de los archivos del sistema y luego compararla con el estado actual del sistema para detectar cualquier cambio.

Aplicativos Web

- **Tripwire:** es una herramienta de integridad de archivos de código abierto. Se utiliza para monitorear los cambios en los archivos y directorios en el sistema. Tripwire puede utilizarse para detectar cambios malintencionados en los archivos y para alertar al usuario en caso de cambios no autorizados. Tripwire es una herramienta esencial para la detección de intrusiones.

- **Monitorix:** Es una herramienta de monitorización de sistemas y redes. Proporciona información en tiempo real sobre el uso de CPU, memoria, disco y red. También incluye gráficos y alertas para ayudar a identificar problemas.

- **Nagios:** Es una herramienta de monitoreo de red de código abierto que se utiliza para monitorear la disponibilidad y el rendimiento de los equipos y servicios en la red. Nagios puede utilizarse para enviar alertas cuando se detectan problemas y para llevar un registro del tiempo de actividad y el rendimiento de los equipos y servicios. Nagios es muy configurable y puede utilizarse para monitorear cualquier tipo de equipo o servicio.

- **Elastic Stack:** es una suite de herramientas que incluye Elasticsearch, Logstash y Kibana, que permiten recopilar, almacenar y visualizar registros de manera efectiva. Elasticsearch es un motor de búsqueda y análisis de datos en tiempo real, Logstash es una herramienta de procesamiento de registros y Kibana es una plataforma de visualización de datos.

- **Graylog:** Es una plataforma de gestión de registros que permite recopilar, indexar y analizar grandes volúmenes de registros de varias fuentes. Permite realizar búsquedas y análisis avanzados.

- **Zabbix:** Es una solución de monitoreo de código abierto que permite la supervisión en tiempo real de servidores, aplicaciones, redes y dispositivos. En el ámbito de la ciberseguridad, Zabbix es crucial para detectar anomalías en el rendimiento del sistema y la red, que podrían indicar intentos de intrusión, ataques DDoS, o actividades maliciosas. Zabbix también permite configurar alertas automáticas basadas en umbrales específicos, lo que ayuda a los administradores de seguridad a responder rápidamente ante posibles incidentes. Además, su capacidad de integración con otras herramientas de seguridad amplía su utilidad para la gestión proactiva de la infraestructura.

- **Cacti:** Es una herramienta de código abierto diseñada para la visualización y almacenamiento de datos de rendimiento de la red, utilizando gráficos generados por RRDTool. En ciberseguridad, Cacti es útil para la monitorización continua de la infraestructura de red, permitiendo a los administradores visualizar patrones de tráfico que podrían indicar actividades sospechosas, como el escaneo de puertos, intentos de exfiltración de datos, o tráfico no autorizado. Al analizar estas tendencias a lo largo del tiempo, Cacti ayuda a identificar comportamientos anómalos y facilita la implementación de medidas preventivas o correctivas para asegurar la red.

d) Análisis de bitácora

Un analizador de bitácoras del sistema es una herramienta que revisa los archivos de registro del sistema para identificar actividades maliciosas o sospechosas.

- **Rsyslog:** Es un sistema de registro de eventos de alta rendimiento y confiable para sistemas Linux. Permite la recolección, procesamiento y envío de registros de diferentes fuentes a diferentes destinos. Rsyslog puede ser configurado para enviar registros a un servidor centralizado o a una base de datos para su posterior análisis y monitoreo. Además, ofrece capacidades de filtrado y enriquecimiento de registros para facilitar la búsqueda y el análisis de datos.

- **Syslog-ng:** Es una herramienta de software libre que se utiliza para recolectar, procesar y almacenar registros de eventos (logs) generados por los sistemas y aplicaciones en un sistema informático. Syslog-ng se ejecuta en sistemas operativos tipo Unix y puede ser configurado para enviar los registros a diferentes destinos, como bases de datos, archivos de texto plano, servidores remotos de syslog, etc.

- **Logwatch:** es una herramienta que revisa diariamente los registros de actividad del sistema y los envía por correo electrónico al administrador. Puede personalizarse para mostrar los registros que se deseen.

- **Logrotate:** es una herramienta que administra los registros del sistema, eliminando los archivos de registro antiguos y archivando los nuevos. Puede ser configurado para comprimir y rotar registros de

  manera automática.

- **grep:** es una herramienta de búsqueda que permite encontrar líneas que contengan un patrón específico en un archivo o en una secuencia de archivos. Se utiliza con frecuencia para buscar errores en los archivos de bitácora. Por ejemplo, grep "error" /var/log/syslog buscará todas las líneas en el archivo /var/log/syslog que contengan la palabra "error".

- **head:** muestra las primeras líneas de un archivo. Es útil para obtener una vista previa rápida de los contenidos de un archivo de registro sin tener que abrir todo el archivo. Por ejemplo, head /var/log/syslog mostrará las primeras diez líneas del archivo /var/log/syslog.

- **tail:** muestra las últimas líneas de un archivo. Se utiliza para obtener las últimas entradas en un archivo de bitácora en tiempo real. Por ejemplo, tail -f /var/log/syslog mostrará las últimas líneas del archivo /var/log/syslog en tiempo real a medida que se agregan.

- **cut:** permite recortar una sección de un archivo de bitácora. Se utiliza con frecuencia para extraer información específica de un archivo de bitácora. Por ejemplo, cut -d " " -f 1,4 /var/log/syslog extraerá el primer y cuarto campo del archivo /var/log/syslog, utilizando un espacio como delimitador.

- **sort:** ordena las líneas de un archivo de bitácora en orden alfabético o numérico. Es útil para organizar los registros de bitácora en un formato más legible. Por ejemplo, sort /var/log/syslog ordenará el archivo /var/log/syslog en orden alfabético.

- **Fluentd:** Es un recolector y procesador de registros que permite la recopilación de registros de varias fuentes, la transformación y enrutamiento de los mismos y su almacenamiento en diferentes destinos.

Para actividades Reactivas

a) Gestión de intrusiones

- **Fail2ban:** Es una herramienta de prevención de intrusiones basada en host (HIPS) que monitorea los registros de autenticación y otros archivos de registro del sistema para detectar intentos fallidos repetidos de acceso o actividades sospechosas. Si Fail2ban detecta un patrón de actividad maliciosa

(como múltiples intentos fallidos de inicio de sesión), bloquea la dirección IP ofensiva mediante la modificación de las reglas del firewall, evitando así ataques de fuerza bruta y otras amenazas. Es especialmente útil en servidores y sistemas expuestos a internet, brindando una capa adicional de seguridad de forma automatizada.

- **Snort:** Es un sistema de detección y prevención de intrusiones en red (NIDS/NIPS) de código abierto que analiza el tráfico de red en tiempo real para identificar patrones y firmas de actividades maliciosas, como intentos de explotación de vulnerabilidades, escaneos de puertos, ataques DDoS, y más. Snort utiliza una combinación de análisis basado en firmas, análisis de protocolos y detección de anomalías para identificar y alertar sobre posibles amenazas, permitiendo a los administradores de red tomar acciones para mitigar los riesgos.

- **Snortsam:** Es una extensión de Snort que permite la integración de Snort con diferentes sistemas de firewall para bloquear automáticamente el tráfico malicioso identificado por Snort. Snortsam funciona interceptando las alertas de Snort y traduciéndose en reglas de firewall que bloquea dinámicamente las direcciones IP involucradas en actividades sospechosas. Esta capacidad de respuesta activa ayuda a contener y mitigar amenazas de manera rápida y efectiva, protegiendo la red en tiempo real.

- **OSSEC:** Es una plataforma de seguridad de código abierto que funciona como un sistema de detección de intrusiones basado en host (HIDS). OSSEC realiza monitoreo de archivos, análisis de registros, y detección de rootkits, además de la correlación de eventos y la respuesta automática ante incidentes. En ciberseguridad, OSSEC es fundamental para la protección proactiva de los sistemas al detectar y alertar sobre cambios no autorizados en archivos críticos, intentos de escalada de privilegios, y otras actividades sospechosas que podrían indicar una intrusión o ataque.

- **Suricata:** Es un motor de inspección de red de código abierto que actúa como un sistema de detección y prevención de intrusiones (IDS/IPS), con la capacidad de realizar monitoreo de red, captura de paquetes, y análisis en profundidad de protocolos. Suricata se destaca por su capacidad de manejar grandes volúmenes de tráfico y por su soporte para la inspección multicapa, permitiendo identificar amenazas tanto en la capa de red como en la capa de aplicación. Además, Suricata es compatible con las reglas de Snort, lo que facilita la transición para los usuarios de Snort y permite la implementación de un enfoque de defensa en profundidad en la infraestructura de red.

- **Wazuh:** Es una plataforma de seguridad de código abierto que proporciona monitoreo en tiempo real, detección de amenazas, y respuesta ante incidentes. Wazuh combina las funcionalidades de un SIEM (Security Information and Event Management) con un HIDS (Host-based Intrusion Detection System), ofreciendo una solución integral para la gestión de la seguridad en sistemas de TI. Es utilizado para la supervisión de la integridad de archivos, análisis de registros, y detección de comportamientos anómalos en los sistemas.

- **Security Onion:** Es una plataforma de código abierto para la monitorización, detección y respuesta ante amenazas (MDR) que integra una variedad de herramientas de ciberseguridad en un entorno centralizado. Security Onion está diseñado para facilitar la implementación de capacidades avanzadas de defensa en redes, como la detección de intrusiones, análisis de tráfico de red y respuesta ante incidentes.

- **Detección de intrusiones:** Integra herramientas como Suricata y Zeek (anteriormente conocido como Bro) para la detección de intrusiones en la red. Estas herramientas analizan el tráfico de red en tiempo real para identificar patrones de comportamiento malicioso o anómalo.

- **Análisis de Logs:** Utiliza Elastic Stack (Elasticsearch, Logstash, Kibana) para la recolección, indexación y visualización de logs y datos de eventos. Esto permite a los analistas correlacionar eventos de diferentes fuentes y obtener una visión completa de la actividad en la red.

- **Análisis Forense:** Incluye herramientas para la captura y análisis de paquetes de red, permitiendo a los equipos de respuesta a incidentes realizar un análisis forense detallado después de un incidente de seguridad. Moloch (Arkime) es una de las herramientas que pueden integrarse para realizar este tipo de análisis.

- **Monitoreo de Host:** A través de la integración con OSSEC, Security Onion también ofrece capacidades de detección de intrusiones en host (HIDS), lo que permite monitorear la integridad de los sistemas y detectar comportamientos sospechosos a nivel de host.

- **Respuesta a Incidentes:** Security Onion no solo se enfoca en la detección, sino que también incluye herramientas para la respuesta a incidentes, ayudando a los equipos de seguridad a tomar decisiones informadas y ejecutar acciones para contener y remediar las amenazas.

b) Antimalware

- **Arkime (antes llamado Moloch):** Es una plataforma de captura y análisis de paquetes de red de código abierto diseñada para la supervisión y análisis forense del tráfico de red a gran escala. En el contexto de ciberseguridad, Arkime es invaluable para realizar un análisis detallado de las comunicaciones de red, permitiendo a los analistas investigar incidentes de seguridad, como brechas de datos, intrusiones, o actividades sospechosas.

  Arkime almacena los paquetes capturados en un formato optimizado y los indexa, facilitando búsquedas rápidas y el análisis de eventos específicos en la red. Además, su capacidad para integrarse con otras herramientas de seguridad y su soporte para consultas avanzadas lo convierten en una herramienta potente para los equipos de respuesta a incidentes y análisis forense.

- **Cuckoo:** Es un sistema de análisis de malware de código abierto. Utiliza máquinas virtuales para analizar archivos y detectar posibles amenazas. Kuckoo es capaz de ejecutar malware en un entorno controlado y analizar su comportamiento para detectar posibles amenazas.

- **Malware Analysis Lab:** es un entorno controlado y seguro diseñado específicamente para analizar y estudiar el comportamiento de malware. En este laboratorio, los analistas de seguridad pueden ejecutar, observar y descomponer muestras de software malicioso para comprender sus mecanismos de funcionamiento, vectores de ataque y objetivos. El laboratorio está completamente aislado del resto de la red para evitar cualquier propagación accidental del malware. Incluye una variedad de herramientas para análisis estático (inspección del código sin ejecutarlo) y dinámico (ejecución del malware para observar su comportamiento). Ejemplos de estas herramientas son IDA Pro, Ghidra (análisis estático), Cuckoo Sandbox, y Remnux (análisis dinámico).

  El laboratorio puede registrar todas las acciones del malware, como las conexiones de red que intenta establecer, los archivos que crea o modifica, y las claves de registro que altera. Proporciona herramientas para desempaquetar y desofuscar el código, ya que los autores de malware a menudo utilizan técnicas para dificultar su análisis. Permite el uso de técnicas de ingeniería inversa para descompilar o desensamblar el malware y estudiar su código fuente.

c) Informática forense

- **SleuthKit Autopsy:** Es una herramienta de análisis forense que permite examinar sistemas de archivos y recuperar datos de discos duros, particiones y sistemas de archivos.

- **Santoku Linux:** Es una distribución de Linux especializada en análisis forense y pruebas de penetración. Incluye herramientas como Nmap, Wireshark, Metasploit,entre otras.

- **Android Debug Bridge (ADB):** Es una herramienta de línea de comandos que permite a los desarrolladores de Android comunicarse con dispositivos Android y emuladores desde un sistema operativo host. Se utiliza para depurar aplicaciones de Android, instalar aplicaciones y controlar dispositivos de forma remota.

Para actividades Retrospectivas

No hemos encontrado herramientas de software libre específicamente diseñadas para actividades retrospectivas. Sin embargo, estas funcionalidades se encuentran distribuidas entre las herramientas mencionadas en los capítulos anteriores. Las herramientas descritas abarcan una gama de funciones preparativas, preventivas, detectivas y reactivas que, en conjunto, pueden ser utilizadas para realizar evaluaciones y análisis retrospectivos efectivos.

3. CONCLUSIONES

La ciberseguridad es un tema crucial en la era digital en la que vivimos, y el software libre ha demostrado ser una herramienta valiosa en este campo. La comunidad de software libre ha creado y mantenido herramientas para preparación, prevención, detección y reacción que son esenciales para la protección de sistemas y redes.

El software libre ha demostrado ser una alternativa viable y poderosa para la ciberseguridad. Sin embargo, es importante recordar que el hecho de que un software esté protegido por una licencia de código abierto no es garantía de calidad o seguridad. Es fundamental revisar la actividad de la comunidad, como las conversaciones y la generación de nuevas versiones con corrección de errores y nuevas funcionalidades, para asegurarnos de la calidad y seguridad del software que utilizamos.

SOBRE EL AUTOR

Ingeniero, empresario y docente enfocado en el sector de la tecnología de información y comunicaciones, con más de 30 años de experiencia en desarrollo de software seguro, seguridad de la información, el uso de estándares de comunicación y la óptima integración del software libre en las organizaciones.

Actualmente se desempeña como gerente de Skina IT Solutions y complementa su vida profesional como profesor de cátedra en la Universidad Javeriana, representando a Colombia en el comité de ciberseguridad de la UPADI.

- Magíster en Ingeniería de Sistemas y Computación Universidad de los Andes, Bogotá, 1998.
- Ingeniero Civil Universidad de los Andes, Bogotá, 1995.
- Diplomado Docencia en Ingeniería Pontificia Universidad Javeriana, Bogotá, 2008

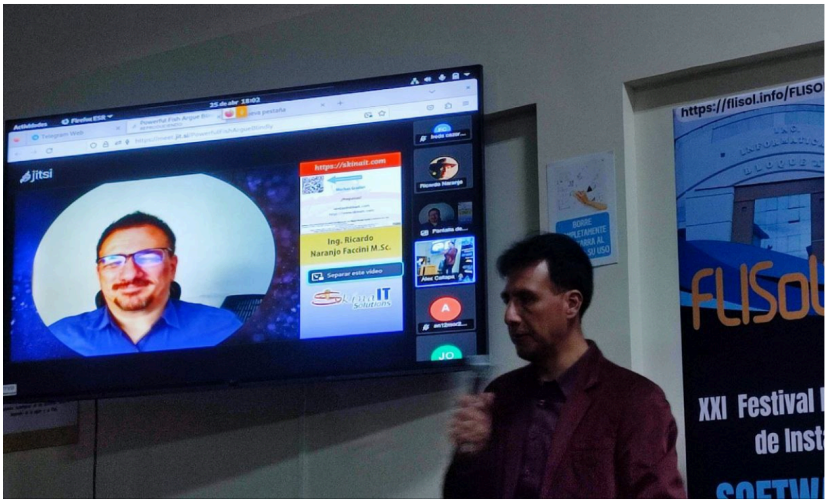

Figura 1: Fotografía de presentación de la ponencia