

# CARÁTULA

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ**

**MANUEL FÉLIX LÓPEZ**

**DIRECCIÓN DE POSGRADO Y EDUCACIÓN CONTINUA**

**INFORME DE LA APLICACIÓN DEL ESTUDIO DE CASO PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER**

**MODALIDAD: EXAMEN DE CARÁCTER COMPLEXIVO**

**TEMA:**

**CENTRO DE OPERACIONES DE SEGURIDAD**

**INFORMÁTICA SOC**

**AUTOR: JUAN CARLOS CEDEÑO REINA**

**TUTORA:**

**MGTR. JESSICA JOHANNA MORALES CARRILLO**

**CALCETA, ABRIL 2022**

# DERECHOS DE AUTORÍA

**JUAN CARLOS CEDEÑO REINA**, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su Reglamento.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**JUAN CARLOS CEDEÑO REINA**

# CONTENIDO GENERAL

[CARÁTULA i](#_Toc100078747)

[DERECHOS DE AUTORÍA ii](#_Toc100078748)

[CONTENIDO GENERAL iii](#_Toc100078749)

[TABLA DE ILUSTRACIONES v](#_Toc100078750)

[CAPÍTULO I. INTRODUCCIÓN DEL INFORME ESCRITO 1](#_Toc100078751)

[CAPÍTULO II. METODOLOGÍA 3](#_Toc100078752)

[2.1. CREACIÓN Y CONFIGURACIÓN DEL ESCENARIO VIRTUAL 3](#_Toc100078753)

[2.2. INSTALCIÓN Y CONFIGURACIÓN DE LA HERRAMIENTA MALTRAIL 3](#_Toc100078754)

[2.3. PRUEBAS PARA EL ANÁLISIS DE TRÁFICO MALICIOSO CON MALTRAIL 3](#_Toc100078755)

[CAPÍTULO III. RESULTADOS Y DISCUSIÓN 4](#_Toc100078756)

[3.1. CREACIÓN Y CONFIGURACIÓN DEL ESCENARIO VIRTUAL 4](#_Toc100078757)

[3.2. INSTALACIÓN Y CONFIGURACIÓN DE LA HERRAMIENTA MALTRAIL 5](#_Toc100078758)

[3.3. PRUEBAS PARA EL ANÁLISIS DE TRÁFICO MALICIOSO CON MALTRAIL 5](#_Toc100078759)

[CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 7](#_Toc100078760)

[4.1. CONCLUSIÓN 7](#_Toc100078761)

[4.2. RECOMENDACIÓN 7](#_Toc100078762)

[BIBLIOGRAFÍA 8](#_Toc100078763)

[ANEXOS 10](#_Toc100078764)

[ANEXO 1. CASO PRÁCTICO DE APLICACIÓN PARA EXAMEN COMPLEXIVO 11](#_Toc100078765)

[ANEXO 2. ARQUITECTURA DEL ESCENARIO VIRTUAL 12](#_Toc100078766)

[AGREGAR ADAPTADORES DE RED EN VIRTUALBOX 12](#_Toc100078767)

[ ADAPTADOR DE RED WAN 12](#_Toc100078768)

[ ADAPTADOR DE RED LAN 13](#_Toc100078769)

[CONFIGURACION DE LOS ADAPTADORES DE RED, MODO NAT PARA EL SISTEMA OPERATIVO DEBIAN11 13](#_Toc100078770)

[ANEXO 3. EJECUCIÓN DEL CASO PRÁCTICO 15](#_Toc100078771)

[CONFIGURACIÓN E INSTALACIÓN DE MALTRAIL 15](#_Toc100078772)

[ INSTALACIÓN DE PAQUETES 15](#_Toc100078773)

[ INSTALACIÓN TMUX 16](#_Toc100078774)

[ CAMBIAR CREDENCIALES DE AUTENTIFICACION PARA EL CLIENTE WEB 18](#_Toc100078775)

[ HABILITAR COMUNICACIÓN SSL EN MALTRAIL 19](#_Toc100078776)

[ DETENER LAS INSTANCIAS DE SENSOR Y SERVER 20](#_Toc100078777)

[INTERFAZ DE INFORMES 20](#_Toc100078778)

[ EVENTOS MOSTRADOS 21](#_Toc100078779)

[ EVENTOS REGISTRADOS EN FORMA DE TABLA 23](#_Toc100078780)

[ANEXO 4 25](#_Toc100078781)

[ANÁLISIS REALIZADOS CON LA HERRAMIENTA MALTRAIL 25](#_Toc100078782)

[ DETALLES DE LA AMENAZA 25](#_Toc100078783)

[ BÚSQUEDA DE DNS INVERSA 25](#_Toc100078784)

[ DETECCIÓN DE ESCANEOS MASIVOS 25](#_Toc100078785)

[ ESCANEO DE DOMINIO DINÁMICO 25](#_Toc100078786)

[ FILTRADO DE DESCARGAS DIRECTAS DE ARCHIVOS 26](#_Toc100078787)

[ TABLERO DE INFORME PARA EL CLIENTE 26](#_Toc100078788)

# TABLA DE ILUSTRACIONES

[**Figura 1.** Escenario virtual 17](#_Toc96704751)

[**Figura 2.** Habilitar adaptador de red para WAN 17](#_Toc96704752)

[**Figura 3.** Habilitar adaptador de red para la LAN 18](#_Toc96704753)

[**Figura 4.** Configuración del adaptador de red 18](#_Toc96704754)

[**Figura 5.** Configuración retransmisión de los paquetes 19](#_Toc96704755)

[**Figura 6.** Permitir comunicación mediante el enmascaramiento IP 19](#_Toc96704756)

[**Figura 7.** Nueva sesión sensor 21](#_Toc96704757)

[**Figura 8.** Compilar el sensor 22](#_Toc96704758)

[**Figura 9.** Nueva sesión server 22](#_Toc96704759)

[**Figura 10.** Compilar el server 22](#_Toc96704760)

[**Figura 11.** Listar las sesiones que están activas tmux 22](#_Toc96704761)

[**Figura 12.** Ingresar a la sesión activa 23](#_Toc96704762)

[**Figura 13.** Obtener la ip del servidor 23](#_Toc96704763)

[**Figura 14.** Interfaz de autenticación 23](#_Toc96704764)

[**Figura 15.** Generar clave sha256 23](#_Toc96704765)

[**Figura 16.** Cambiar la clave en el archivo de configuración 24](#_Toc96704766)

[**Figura 17.** Ingresar al archivo de configuración 24](#_Toc96704767)

[**Figura 18.** Habilitar SSL 24](#_Toc96704768)

[**Figura 19.** Instalar el soporte SSL para python 24](#_Toc96704769)

[**Figura 20.** Crear certificado 25](#_Toc96704770)

[**Figura 21.** Descomentar las líneas 25](#_Toc96704771)

[**Figura 22.** Líneas descomentadas 25](#_Toc96704772)

[**Figura 23.** Ejecución del server para realizar los cambios 25](#_Toc96704773)

[**Figura 24.** Interfaz usuario 26](#_Toc96704774)

[**Figura 25.** Eventos pasados 26](#_Toc96704775)

[**Figura 26.** Gráfica de eventos 27](#_Toc96704776)

[**Figura 27.** Gráfico de números de eventos 27](#_Toc96704777)

[**Figura 28.** Gráfico de las principales amenazas 28](#_Toc96704778)

[**Figura 29.** Grafico ataques provenientes del exterior 28](#_Toc96704779)

[**Figura 30.** Representación en forma de tabla 28](#_Toc96704780)

[**Figura 31.** Detalle de las amenazas 30](#_Toc96704781)

[**Figura 32.** Búsqueda inversa de DNS 30](#_Toc96704782)

[**Figura 33.** Detección de escaneos masivos 30](#_Toc96704783)

[**Figura 34.** Escaneo de dominio dinámico 31](#_Toc96704784)

[**Figura 35.** Filtrado de descarga directa 31](#_Toc96704785)

[**Figura 36.** Tabla de análisis 31](#_Toc96704786)

# CAPÍTULO I. INTRODUCCIÓN DEL INFORME ESCRITO

Según un informe reciente, la cantidad promedio de brechas de seguridad reportadas por las organizaciones aumentó un 11%, de 130 en 2017 a 145 incidentes en 2018 (Bissell & Ponemon, 2018). En los últimos cinco años, este número ha aumentado en un total del 65%. Sin embargo, este informe sólo cubre los incidentes detectados y notificados, y el número de incidentes no notificados es probablemente mucho mayor.

Los centros de operaciones de seguridad (SOC) pueden proporcionar una solución integral para detectar y mitigar un ataque si se implementan correctamente. Sin embargo, amenazas colosales, complejas e indeterminadas en el mundo cibernético. Los ciberataques están sucediendo a diario y podrían lanzarse contra una red empresarial en cualquier momento, cada vez más organizaciones han establecido Centros de Operaciones de Seguridad (SOC) para coordinar las defensas contra los ciberataques (Jarpey & McCoy, 2017).

El coste total anual de cualquier tipo de ciberataques también crece a un ritmo constante. Desafortunadamente, muchos ataques son provocados por código malicioso, comúnmente llamado "malware", que muestra de forma persistente uno de los mayores problemas de ciberseguridad para las empresas (Janampa Patilla, Huamani Santiago, & Meneses Conislla, 2021). La infección por software malicioso puede estar presentes en organizaciones de todo tipo debido a factores que pueden ser por influencias internas o externas, que hace incierto saber cuándo se lleve a cabo un ataque a nivel de red el cual puede provocar consecuencias al sistema de información (Brito, 2018). Los diferentes tipos de ataques de los ciberdelincuentes no sólo afectan a las grandes empresas, sino también a las pequeñas y medianas empresas, este tipo de software extremadamente malicioso se ha convertido en una sofisticada, herramienta cosechando miles de millones de dólares en ganancias (Alenezi, Alabdulrazzaq, Alshaher, & Alkharang, 2020), por ejemplo el Ransomware de cifrado impiden a los usuarios acceder al sistema o sus archivos y obliga a que se efectué un pago para descifrar su información.

Cuando ocurre un incidente de seguridad, las tres preguntas principales que un SOC busca responder son: ¿Qué ha ocurrido el ataque? ¿Por qué sucedió? ¿Qué acción se debe hacer? Mientras que una variedad de software herramientas (p. ej., sistema de gestión de información de seguridad, sistemas de seguridad basados en host) y hardware equipos (por ejemplo, sistemas de detección de intrusos en la red) el cual permite detectar y correlacionar eventos relacionados con la seguridad (Miloslavskaya, Tolstoy, & Zapechnikov, 2016), los SOC del mundo real aún dependen de la seguridad analistas (y oficiales de vigilancia) para tomar decisiones sobre "¿Qué debo hacer?". Debido a que los SOC aún no han adoptado una respuesta de intrusión autónoma (Ganame, Bourgeois, Bidou, & Spies, 2007).

El presente trabajo partió de un caso de estudio en el cual se debe realizar implementación de un Centro de Operaciones de Seguridad Informática SOC, para identificar las anomalías procedentes desde la red WAN y la red LAN, conocer los diferentes protocolos a los cuales viene dirigido el ataque. Tras el desarrollo de la solución se determinó el uso de MalTrail, que es una herramienta que permite la detección de tráfico malicioso, consta principalmente de cuatro componentes Tráfico-Sensor-Cliente-Servidor, utiliza listas negras de código abierto, además, utiliza los datos de los sitios web bloqueados y las direcciones IP de varios proveedores de antivirus, también cuenta con definiciones de virus específicas, es decir, que si ocurre una coincidencia se activa la alerta, la cual realizara él envió de los resultados al servidor local centralizado para poder mostrarlos mediante la interfaz web.

# CAPÍTULO II. METODOLOGÍA

Para el proceso de resolución del caso práctico de un “Centro de Operaciones de Seguridad Informática SOC para identificar las anomalías procedentes desde la rede WAN y la red LAN”, en el que se debe conocer los diferentes protocolos a los cuales viene dirigido el ataque, realizar ataques en ambiente controlado y explicar el por qué, se llevó a cabo el siguiente procedimiento, detallado por etapas:

2.1. CREACIÓN Y CONFIGURACIÓN DEL ESCENARIO VIRTUAL

La máquina virtual se creó mediante el uso de VirtualBox. Se instaló el sistema operativo Debian11 para poder realizar el procedimiento de configuración, compilación de la herramienta MalTrail (Echeto, 2021).

2.2. INSTALCIÓN Y CONFIGURACIÓN DE LA HERRAMIENTA MALTRAIL

Al finalizar el proceso de instalación del sistema operativo Debian11, lo siguiente fue la instalación y configuración de los paquetes necesarios para MalTrail el cual requiere, Python para que pueda ser compilado de forma correcta, al concluir con el proceso de instalación de los paquetes se compiló archivos necesarios para iniciar la herramienta con los servicios server y el sensor.

2.3. PRUEBAS PARA EL ANÁLISIS DE TRÁFICO MALICIOSO CON MALTRAIL

En la fase de pruebas se ejecutó la configuración en un entorno en KaliLinux, que fue el equipo que permitió efectuar el análisis, esto con el propósito de saber si la herramienta está funcionando de forma óptima.

# CAPÍTULO III. RESULTADOS Y DISCUSIÓN

Un Centro de Operaciones de Seguridad SOC para el caso de estudio presentado en este informe, permitió proporcionar una solución integral para detectar y mitigar un ataque. Incorpora una mezcla de personas, procesos y tecnologías para identificar, detectar y mitigar amenazas de manera efectiva, idealmente antes de que ocurra cualquier daño. Los resultados obtenidos en cada etapa de la metodología se detallan a continuación.

3.1. CREACIÓN Y CONFIGURACIÓN DEL ESCENARIO VIRTUAL

La máquina virtual se creó con 4Gb de memoria RAM y un procesador dual core, un disco duro de capacidad 240GB para instalar el sistema. Durante la instalación se agregó la contraseña para el usuario (ROOT) es aquella que tiene todos los permisos y privilegios.

Una de las pruebas realizadas fue evaluar si la configuración de las interfaces en modo NAT, permitan iniciar la comunicación de los dispositivos del interior a través de la interfaz exterior mediante la traducción de su dirección, en la Anexo 2 Figura 1, se presenta la arquitectura de red. Para este procedimiento de evaluación, se conectó un equipo a la interfaz de red interna para comprobar si se obtiene acceso a la red.

Antes de iniciar la máquina, se habilitaron dos interfaces de red una para la red WAN y otra para la LAN (Anexo 2 Figuras 2 y 3) muestra como habilitar los adaptadores de red, en la interfaz para la red WAN externa se le configuró una dirección IP 192.168.1.14, la cual permitió tener acceso a internet desde la máquina virtual, para red LAN interna se le configuró una dirección IP 10.0.0.1 (Anexo 2 Figura 4) se detalla configuración del adaptador en Debían, a continuación se procedió con la configuración de las interfaces en modo NAT para permitir que los equipos internos tengan acceso a la red para poder identificar las anomalías procedentes desde la red WAN y LAN (Anexo 2 Figuras 5 y 6) se explica cómo habilitar retransmisión de paquetes y enmascaramiento IP para realizar el análisis de tráfico de red que proviene desde la red externa como la interna.

3.2. INSTALACIÓN Y CONFIGURACIÓN DE LA HERRAMIENTA MALTRAIL

Para la correcta implementación de la MalTrail, es necesario instalar la librería Python-pcapy para la correcta operatividad del software, la cual se describe en el Anexo 3, que trata sobre: la ejecución del caso práctico, la instalación de los archivos adicionales, las dependencias necesarias para la correcta compilación de la aplicación, el procedimiento que se realizó para cambiar las credenciales del usuario administrador, ingreso a la interfaz web y obtención de todos los eventos registrados que serán transferidos, que permitirá visualizar: amenazas, eventos y rastro.

3.3. PRUEBAS PARA EL ANÁLISIS DE TRÁFICO MALICIOSO CON MALTRAIL

Las pruebas de análisis de tráfico malicioso fueron realizadas en el sistema operativo KaliLinux, el cual permitió realizar prueba de seguridad de la información. Se procedió a realizar las siguientes pruebas: búsqueda de DNS inversa (Anexo 4, Figura 27), detección de escaneos masivos (Anexo 4, Figura 28), escaneo de dominio dinámico (Anexo 4, Figura 29) y filtrado de descargas directas de archivos (Anexo 4 Figura 30) permite visualizar el filtrado de descarga directa, mediante el uso de las siguientes herramientas:

* **Hping3**, esta aplicación permitió enviar paquetes TCP, UDP y RAW-IP.
* **Nmap**, determinó el estado de los objetos en la red escaneada, así como los puertos y sus servicios correspondientes.
* **Nslookup**, permitió acceder al servidor de nombres (NS) desde la línea de comandos. Con su ayuda, puede verificar el funcionamiento del servidor DNS.
* **Sqlmap**, es una herramienta código abierto que automatiza el proceso de encontrar y explotar inyecciones de SQL para extraer datos o hacerse cargo de un host remoto.

Finalizado el análisis de prueba con MalTrail, se puede observar en la tabla de análisis (Anexo 4, Figura 31) en la cual muestra la captura del tráfico malicioso, que se ha realizado mediante el uso de las herramientas mencionadas anteriormente las alertas que se mostraron por el análisis fueron: escaneo de puertos potenciales, agente de usuario mapa SQL y tráfico sospechoso. Los registros obtenidos se presentan en la interfaz web (Anexo 4), la cual permite obtener una comprensión previa de lo que está sucediendo en la red. Para poder tomar las acciones necesaria para lograr mitigar o reducir el impacto del ataque.

# CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIÓN

A partir del resultado y las pruebas realizadas se puede concluir, que el diseño de un sistema de control de tráfico malicioso reducirá el daño a la infraestructura de las amenazas que provienen de Internet o intranet mediante la utilización de listas negras disponibles públicamente. En esta forma de enfoque, se confía en las firmas que el proveedor de AV le da al usuario final. Porque se está actualizando nuestras definiciones con varios informes AV y nuestras definiciones personalizadas para bloquear el contenido. La seguridad de la red es un campo de estudio que ofrece infinitas posibilidades de investigación y desarrollo.

MalTrail se convierte en una herramienta que apoya la gestión de la seguridad de información, en conclusión, el enfoque de esta arquitectura que se centra en la captura de paquetes para el análisis de tráfico malicioso permite conocer de manera rápida cuáles son los detalles de la amenaza, como origen, destino y los puertos de origen, logrando así determinar cuál es la acción a tomar para mitigar o reducir las superficies del ataque y el impacto del tráfico malicioso dentro de una red.

4.2. RECOMENDACIÓN

Es recomendable que se mantengan configuradas las actualizaciones de forma periódica de las listas de informes para que se reconozcan debidamente las amenazas y cambios que se presenten en los equipos de forma cotidiana.

Se recomienda que desde la administración se monitorice el sistema de detección y prevención de tráfico malicioso, de manera que permitan tomar medidas a tiempo en base a cualquier amenaza que eventualmente pueda presentarse.

La capacitación a los usuarios finales es muy importante. Es recomendable que el usuario tome conciencia ante la accesibilidad de la información que fluye en la web y sepan reconocer cuando o no se puede descargar, instalar o administrar algún elemento desde internet para que no se vulnere las seguridades en los equipos.

# BIBLIOGRAFÍA

Bissell, K., & Ponemon, L. (2018). *THE COST OF CYBERCRIME.* New York: Accenture and Ponemon Institute. Recuperado el 11 de Febrero de 2022, de https://www.accenture.com/\_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Brito Gómez, D. (2018). El riesgo empresarial. *Universidad y Sociedad*, 269-277. Obtenido de http://scielo.sld.cu/pdf/rus/v10n1/2218-3620-rus-10-01-269.pdf

Echeto, D. (03 de Marzo de 2021). *msn.com*. Recuperado el 2022 de Febrero de 11, de https://www.msn.com/es-es/noticias/tecnologia/qu%C3%A9-esvirtualbox-y-para-qu%C3%A9-sirve/ar-BB1f4nku

Ganame, A., Bourgeois, J., Bidou, R., & Spies, F. (2007). A Global Security Architecture for Intrusion Detection on Computer Networks. *IEEE*. doi:10.1109/IPDPS.2007.370621

Janampa Patilla, H., Huamani Santiago, H., & Meneses Conislla, Y. (2021). Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. *Revista Cubana de Ciencias Informáticas, 15*(3), 55-73. Recuperado el 5 de Febrero de 2022, de http://scielo.sld.cu/pdf/rcci/v15n3/2227-1899-rcci-15-03-55.pdf

Jarpey, G., & McCoy, R. (2017). *Security Operations Center Guidebook A Practical Guide for a Successful SOC.* Chennai, India: Hilary Carr. Recuperado el 11 de Febrero de 2022, de https://pdfroom.com/preview/books/security-operations-center-guidebook-a-practical-guide-for-a-successful-soc/Pe5xQqMZdnN

Miloslavskaya, N., Tolstoy, A., & Zapechnikov, S. (2016). Taxonomy for Unsecure Big Data Processing in Security Operations Centers. *IEEE*. doi:10.1109/W-FiCloud.2016.42

N. Alenezi, M., Alabdulrazzaq, H., A. Alshaher, A., & M. Alkharang, M. (2020). Evolution of Malware Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security*, 326-337. Recuperado el 04 de Febrero de 2022, de https://www.researchgate.net/profile/Haneen-Alabdulrazzaq/publication/349324759\_Evolution\_of\_Malware\_Threats\_and\_Techniques\_A\_Review/links/602ad0e64585158939a93934/Evolution-of-Malware-Threats-and-Techniques-A-Review.pdf

Redhat. (20 de Junio de 2018). *redhat*. Obtenido de https://www.redhat.com/en/topics/security/what-is-malware

# ANEXOS

# ANEXO 1. CASO PRÁCTICO DE APLICACIÓN PARA EXAMEN COMPLEXIVO



**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ**

**MANUEL FÉLIX LÓPEZ**

DIRECCIÓN DE POSGRADO Y EDUCACIÓN CONTÍNUA

**MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS**

**REGISTRO DE CASO PRÁCTICO DE APLICACIÓN PARA EXAMEN COMPLEXIVO**

**Caso de Estudio: Centro de Operaciones de Seguridad Informática SOC**

**Instrucciones:**

* Identificar las anomalías procedentes desde la rede WAN y la red LAN
* Documente las actividades por pasos

**Detalle del Caso:**

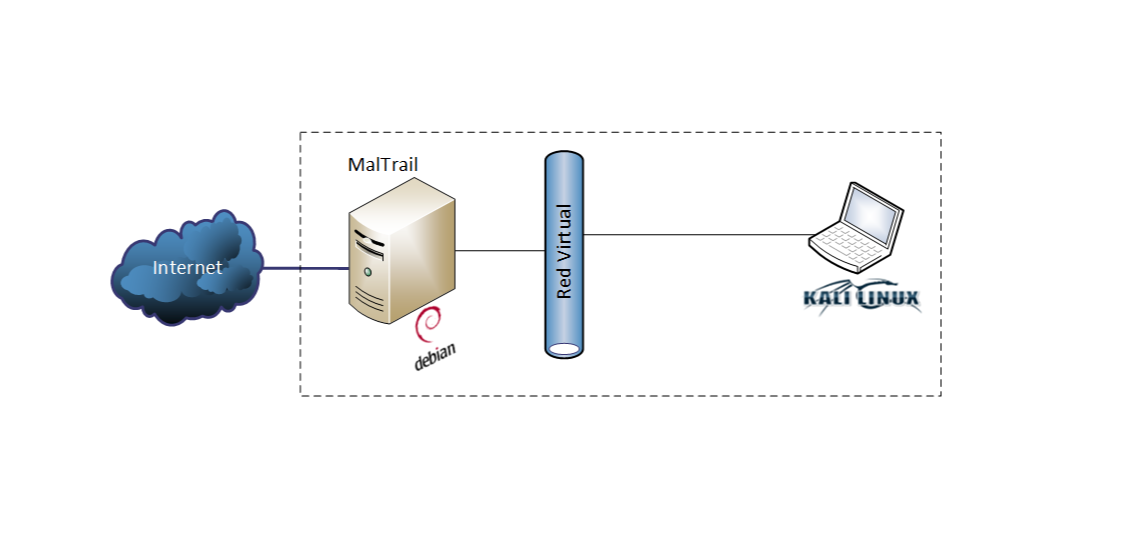
La empresa Cibersect S. A se dedica a brindar servicio de ciberseguridad a nivel nacional. Su principal fortaleza es el despliegue de su sistema de monitoreo y control de incidentes y anomalías presentadas por ciberdelincuentes, para mejorar sus servicios debe realizar un despliegue tecnológico de un SOC para lo cual debe realizar procedimientos de implementación de un Centro de Operaciones de Seguridad Informática SOC.

**Solución:**

Maltrail que es una herramienta que se basa en la arquitectura Tráfico -> Sensor <-> Servidor <-> Cliente. El sensor es un componente independiente que se ejecuta en un host de monitoreo donde "supervisa" el tráfico que pasa en busca de elementos/huellas en la lista negra (es decir, nombres de dominio, URL y/o direcciones IP).

# ANEXO 2. ARQUITECTURA DEL ESCENARIO VIRTUAL

La siguiente imagen muestra la arquitectura que se utilizó en el escenario virtual.

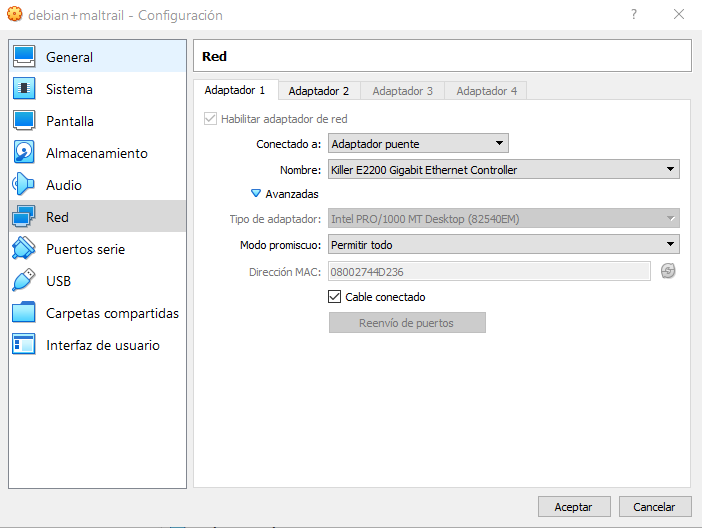


**Figura 1.** Escenario virtual

AGREGAR ADAPTADORES DE RED EN VIRTUALBOX

* ADAPTADOR DE RED WAN

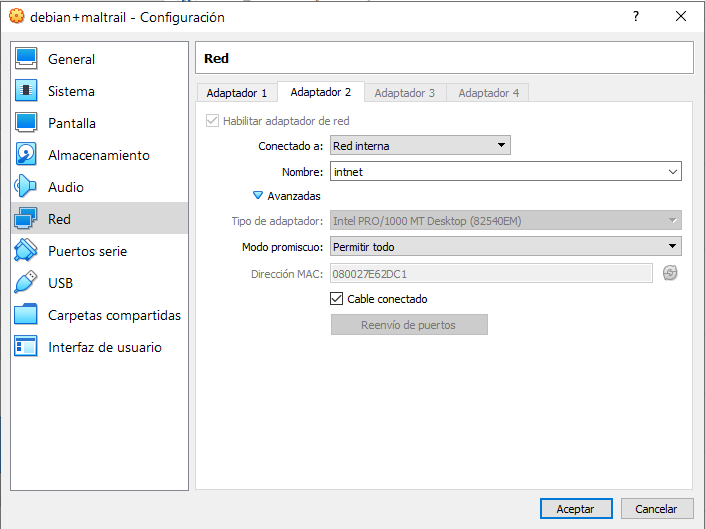
Este tipo de conexión simula la conexión física a la red de la máquina virtual. Este significa que nuestra máquina virtual, estará conectada a través de un adaptador de red creado en la máquina host al router o servidor de nuestro entorno.



**Figura 2.** Habilitar adaptador de red para WAN

* ADAPTADOR DE RED LAN

Este tipo de red permite la comunicación de las máquinas virtuales entre ellas como si de una red LAN se tratase.

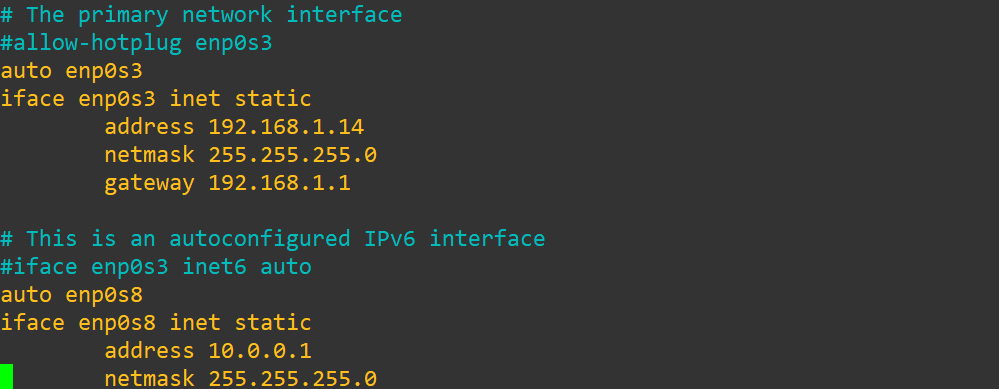


**Figura 3.** Habilitar adaptador de red para la LAN

CONFIGURACION DE LOS ADAPTADORES DE RED, MODO NAT PARA EL SISTEMA OPERATIVO DEBIAN11

A continuación se muestra la configuración para los adaptadores de red WAN y LAN en modo NAT, para realizar este procedimiento se utilizó el siguiente comando como que se muestra a continuación.

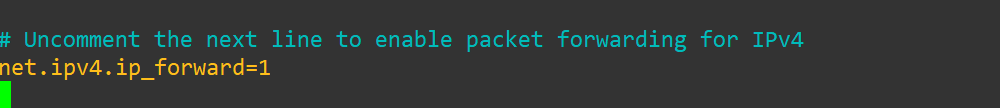
#nano /etc/network/interfaces



**Figura 4.** Configuración del adaptador de red

Lo siguiente fue habilitar “net.ipv4.ip\_forward=1”, que es el mecanismo de “IP forwarding” se encarga de la retransmisión de los paquetes que se reciben por una interfaz física.

#nano /etc/sysctl.conf



**Figura 5.** Configuración retransmisión de los paquetes

Para permitir la comunicación se agregó la regla iptables que permite a los equipos de la LAN que tengan una dirección IP privada comunicarse con redes públicas externas, mediante el enmascaramiento IP.



**Figura 6.** Permitir comunicación mediante el enmascaramiento IP

# ANEXO 3. EJECUCIÓN DEL CASO PRÁCTICO

CONFIGURACIÓN E INSTALACIÓN DE MALTRAIL

La instalación y configuración de MalTrail fue realizada en el sistema operativo Debian11, la cual se ha fundamentado en las recomendaciones realizadas en repositorio oficial de MalTrail [https://github.com/stamparm/maltrail](about:blank).

* INSTALACIÓN DE PAQUETES

Una vez terminado el proceso de instalación de la máquina principal, se instalaron todos los paquetes necesarios para el correcto funcionamiento de MalTrail.

Dentro del equipo principal, inicialmente se instaló los paquetes de Python, ejecutando los siguientes comandos.

El siguiente comando permite clonar el repositorio para luego proceder con la compilación e instalación:

# sudo apt-get install git

En el equipo que permitirá supervisar el tráfico de la red se debe instalar Python con los comandos que se muestran a continuación:

# sudo apt-get install python3

Se procede con la instalación archivos adicionales que necesita para ejecución de Python:

# sudo apt-get install python3-dev python3-pip python-is-python3

A continuación, se instalaran algunas dependencias a continuación se describe para que se utilizan:

# sudo apt-get install libpcap-dev build-essential procps schedtool

* **libpcap-dev:** biblioteca de funciones de captura de paquetes. Se utiliza para capturar paquetes de datos que pasan a través de la interfaz de red especificada.
* **build-essential:** contiene las herramientas necesarias para crear, compilar e instalar programas.
* **procps:** obtiene la información sobre los procesos a través del directorio /proc.
* **schedtool:** puede establecer todos los parámetros de programación de la CPU de los que Linux es capaz o mostrar información para procesos dados.

Se debe instalar Pcapy-NG que es un módulo de extensión de Python que permite que el software escrito en Python acceda a las rutinas de la biblioteca de captura de paquetes pcap:

# sudo pip3 install pcapy-ng

Después de que se finalizó el proceso de instalación. Se procede a clonar maltrail desde la fuente git:

# git clone --depth 1 [https://github.com/stamparm/maltrail.git](about:blank)

* INSTALACIÓN TMUX

Para la instalación de tmux se puede realizar ejecutando el siguiente comando:

# apt-get -y install tmux

Con código que se muestra a continuación se puede crear una nueva sesión nombrada con tmux new:

# tmux new -s sensor

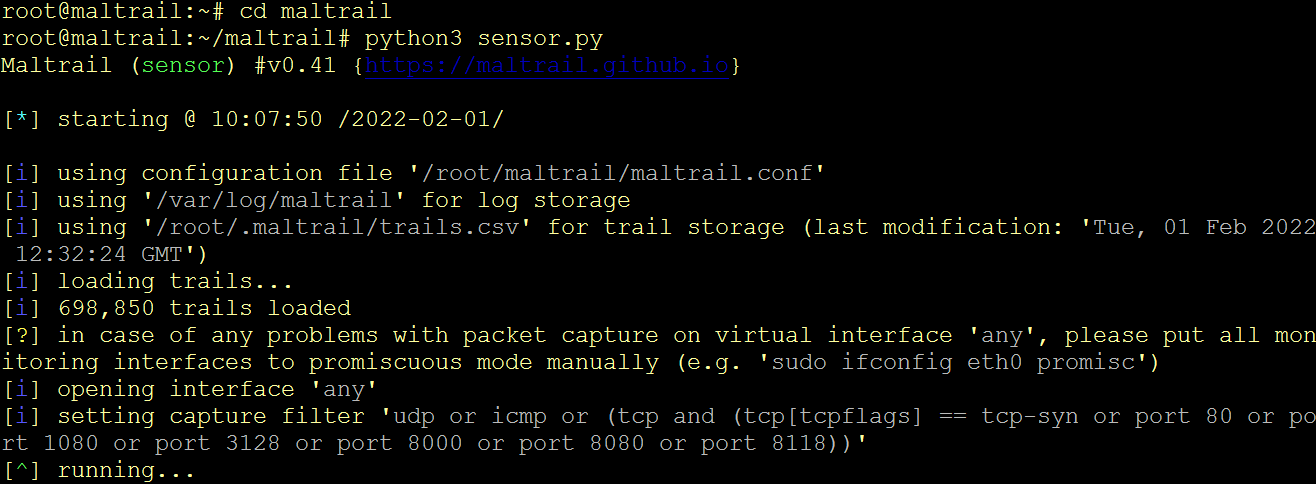


**Figura 7.** Nueva sesión sensor

El cual muestra una terminal adjunta, la cual permitirá compilar el sensor:

# cd maltrail

# python3 sensor.py



**Figura 8.** Compilar el sensor

**Nota:** Para regresar a la teminal principal se presiona la tecla (CTRL+B), luego se presiona la tecla (D).

Se procede a crear la siguiente sesión que permite compilar el server:

# tmux new -s server



**Figura 9.** Nueva sesión server

Se puede proceder con la compilación del server con el siguiente comando:

# cd maltrail

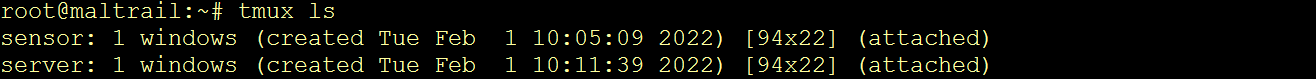
# python3 server.py



**Figura 10.** Compilar el server

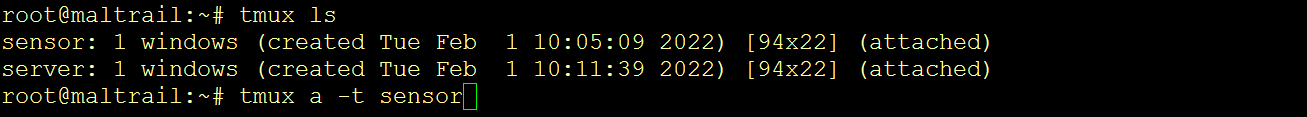
**Nota:** Para regresar a la teminal principal se presiona la tecla (CTRL+B), luego se presiona la tecla (D).

Para ver todas las sesiones, puede ejecutar:



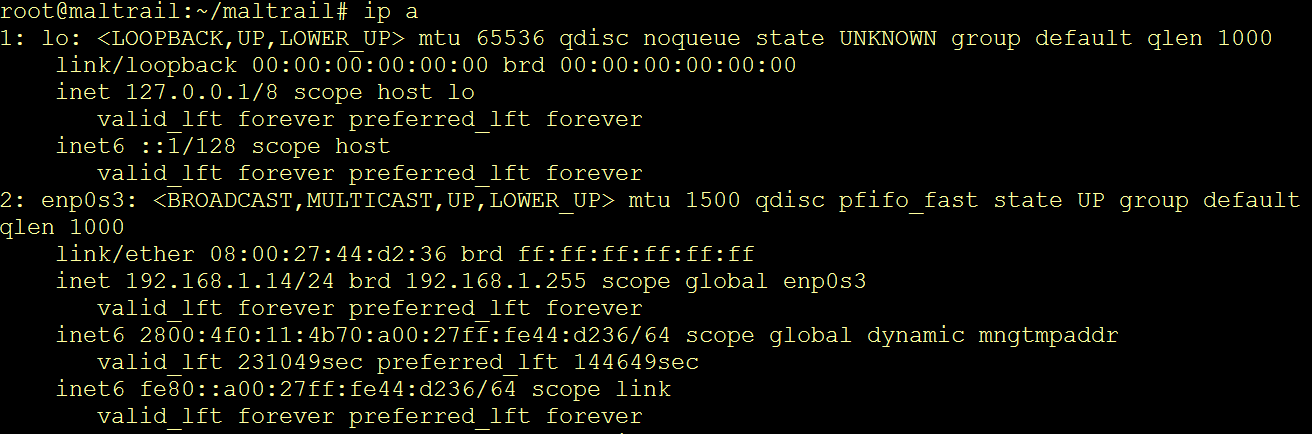
**Figura 11.** Listar las sesiones que están activas tmux

Para volver a conectarse a una sesión, use:

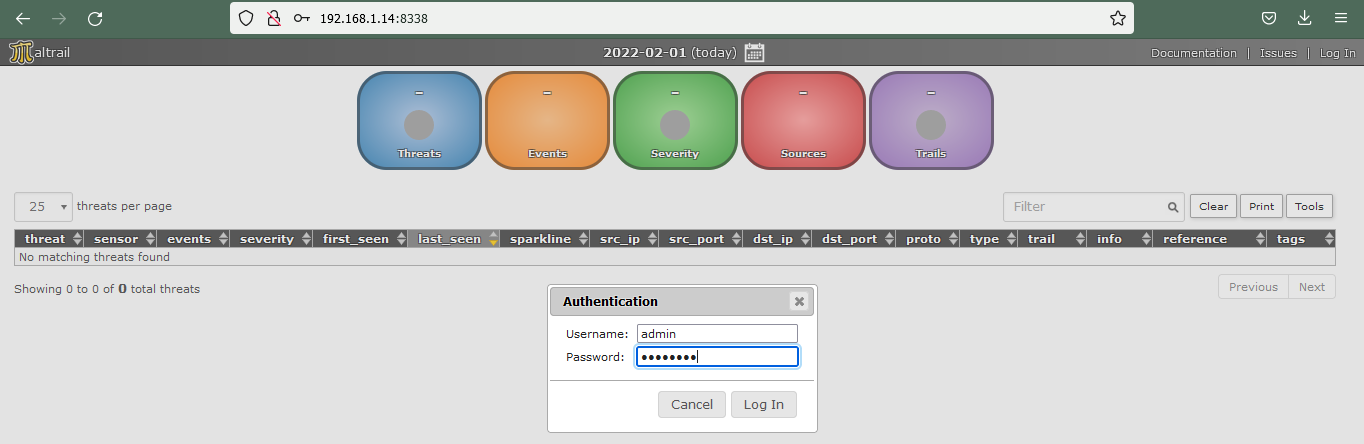


**Figura 12.** Ingresar a la sesión activa

Acceda a la interfaz de informes (es decir, Cliente) visitando http://ipservidor:8338 (credenciales predeterminadas:) admin:changeme! desde su navegador web:



**Figura 13.** Obtener la ip del servidor



**Figura 14.** Interfaz de autenticación

* CAMBIAR CREDENCIALES DE AUTENTIFICACION PARA EL CLIENTE WEB

Para realizar el cambio de credencial para el usuario administrador, debe generar una contraseña sha256 ejecutando el siguiente comando:

# echo -n 'root1234' | sha256sum | cut -d " " -f 1



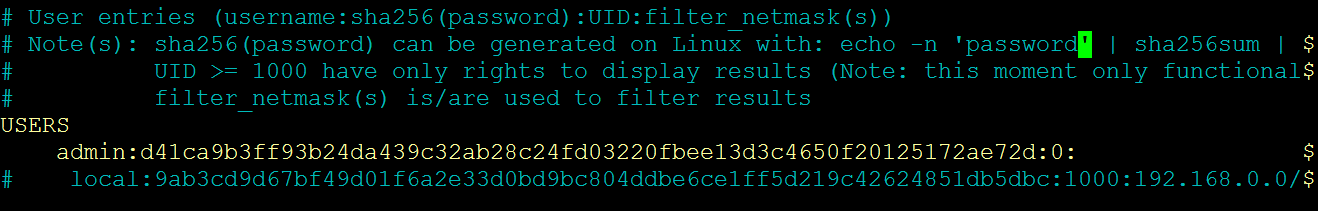
**Figura 15.** Generar clave sha256

A continuación, se copió la cadena cifrada y se pegó en el archivo de configuración maltrail.conf, sección del servidor, subsección USUARIOS. Por ejemplo, si estuviera cambiando para el usuario administrador:

Para realizar las configuraciones de la herramienta MalTrail, se ingresa al directorio donde se encuentra los archivos de compilación ejecutando el siguiente comando:

# cd maltrail

Edite el archivo de configuración mailtrail.conf con nano, busque el apartado users y edite clave cifrada del admin:



**Figura 16.** Cambiar la clave en el archivo de configuración

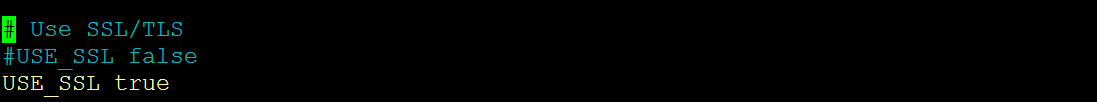
* HABILITAR COMUNICACIÓN SSL EN MALTRAIL

Ingresar al archivo de configuración que se encuentra en el siguiente directorio.



**Figura 17.** Ingresar al archivo de configuración

Se busca en el archivo de configuración la siguiente línea “USE\_SSL”, se encuentra definida en false, se cambia por true.



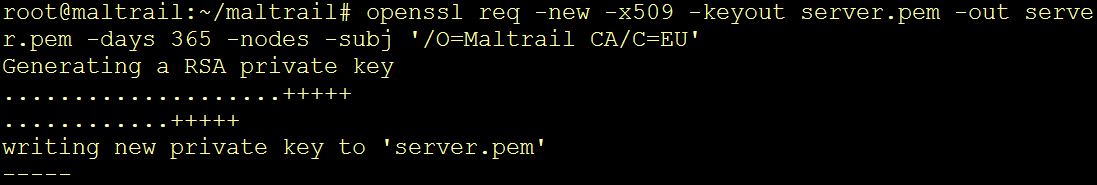
**Figura 18.** Habilitar SSL

Habilitar la comunicación SSL que crean conexiones de servidor o cliente habilita el soporte y configuración del protocolo SSL para instalarlo se realiza con el siguiente comando.



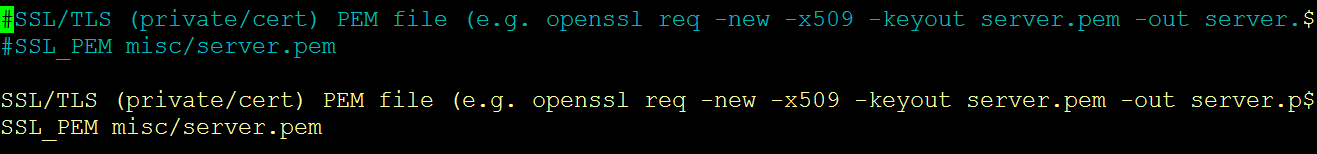
**Figura 19.** Instalar el soporte SSL para Python

Crear la clave para el certificado SSL se realiza con el siguiente comando:



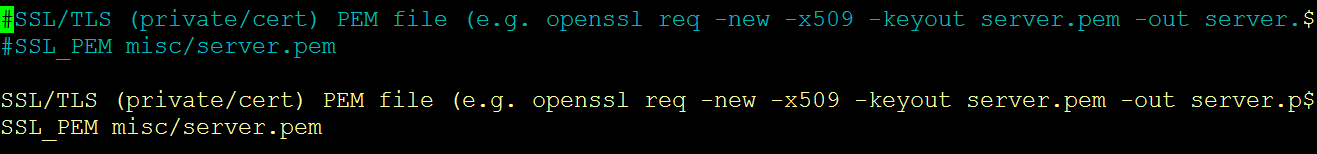
**Figura 20.** Crear certificado

Cuando finalice el proceso del certificado SSL ahora se puede habilitar en el archivo de configuración las siguientes líneas ya que se encuentran comentadas.



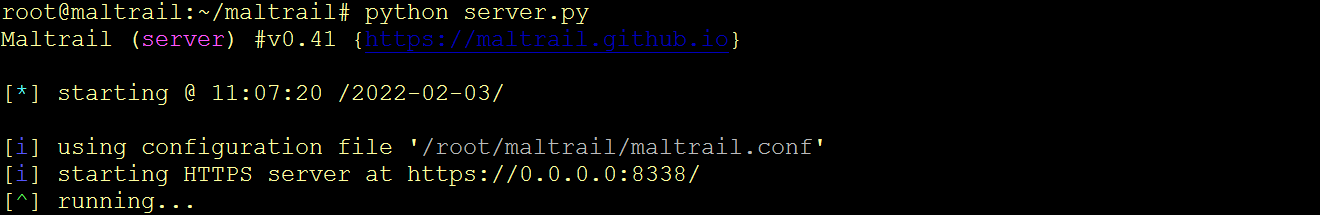
**Figura 21.** Descomentar las líneas

Debe dejarla como se muestra a continuación:



**Figura 22.** Líneas descomentadas

Al ejecutar el server muestra que se habilitó la conexión segura.



**Figura 23.** Ejecución del server para realizar los cambios

Nota: para realizar este procedimiento debe detener el server con el siguiente comando (# pkill -f server.py).

* DETENER LAS INSTANCIAS DE SENSOR Y SERVER

Para detener las instancias del Sensor y Server, se ejecute lo siguiente:

# pkill -f sensor.py

# pkill -f server.py

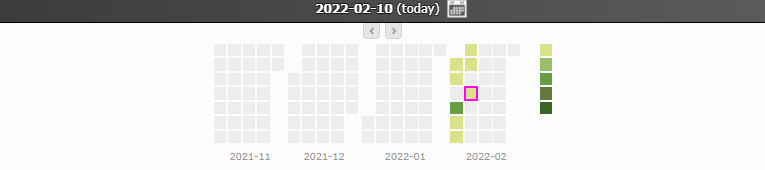
INTERFAZ DE INFORMES

Al ingresar las credenciales adecuadas, muestra la siguiente interfaz de informe:



**Figura 24.** Interfaz usuario

En la parte superior contiene una línea de tiempo deslizante (Nota: se activa después de hacer clic en el ícono de calendario), donde el usuario puede seleccionar registros de eventos pasados. Las fechas se agrupan por meses. Es decir el usuario puede acceder fácilmente a eventos de meses anteriores.



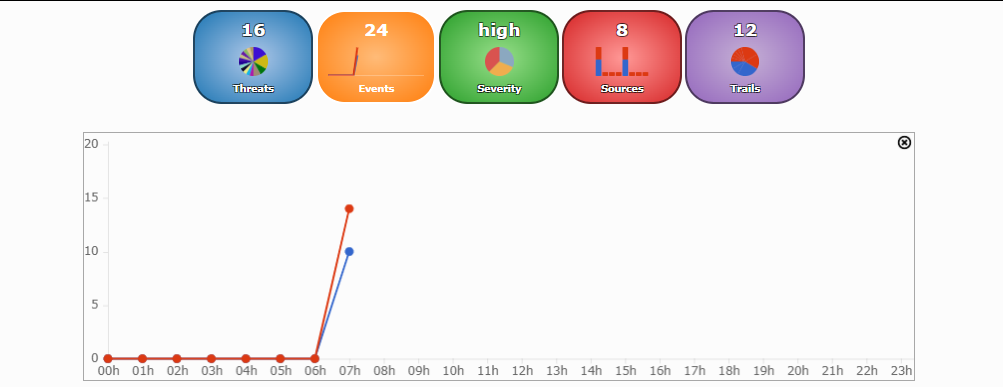
**Figura 25.** Eventos pasados

Al realizar clic sobre la fecha, todos los eventos para esa fecha en particular deben cargarse y representarse en el navegador web del cliente. Según el número de eventos y la velocidad de conexión de la red, la carga y visualización de los eventos registrados puede tardar desde un par de segundos hasta varios minutos.

* EVENTOS MOSTRADOS

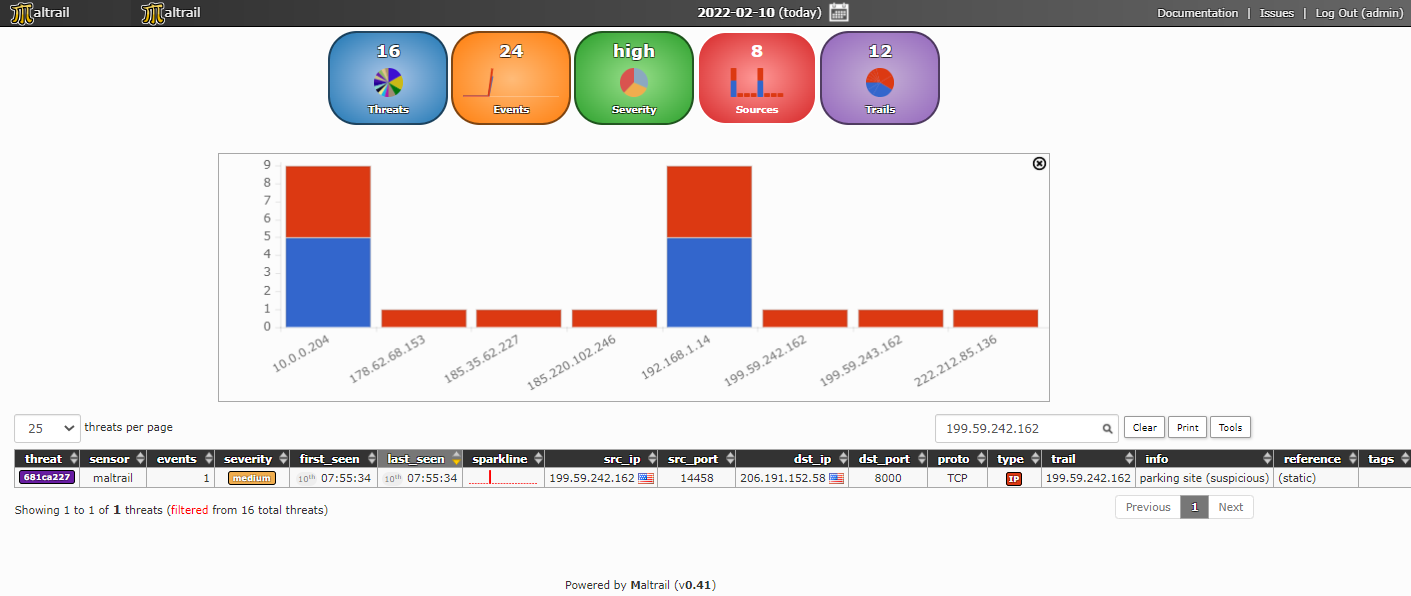
La parte central contiene un resumen de los eventos mostrados a continuación se detalla:

**Events** El cuadro representa el número total de eventos en un período seleccionado de 24 horas, donde la línea roja representa eventos basados ​​en IP, la línea azul representa eventos basados ​​en DNS y la línea amarilla representa eventos basados ​​en URL.



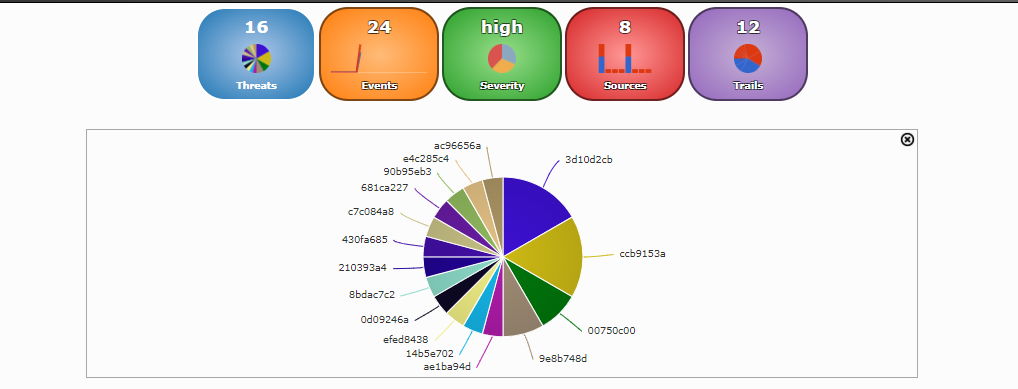
**Figura 26.** Gráfica de eventos

**Sources** El cuadro representa el número de eventos por fuentes principales en forma de un gráfico de columnas apiladas, con el número total de fuentes en la parte superior.



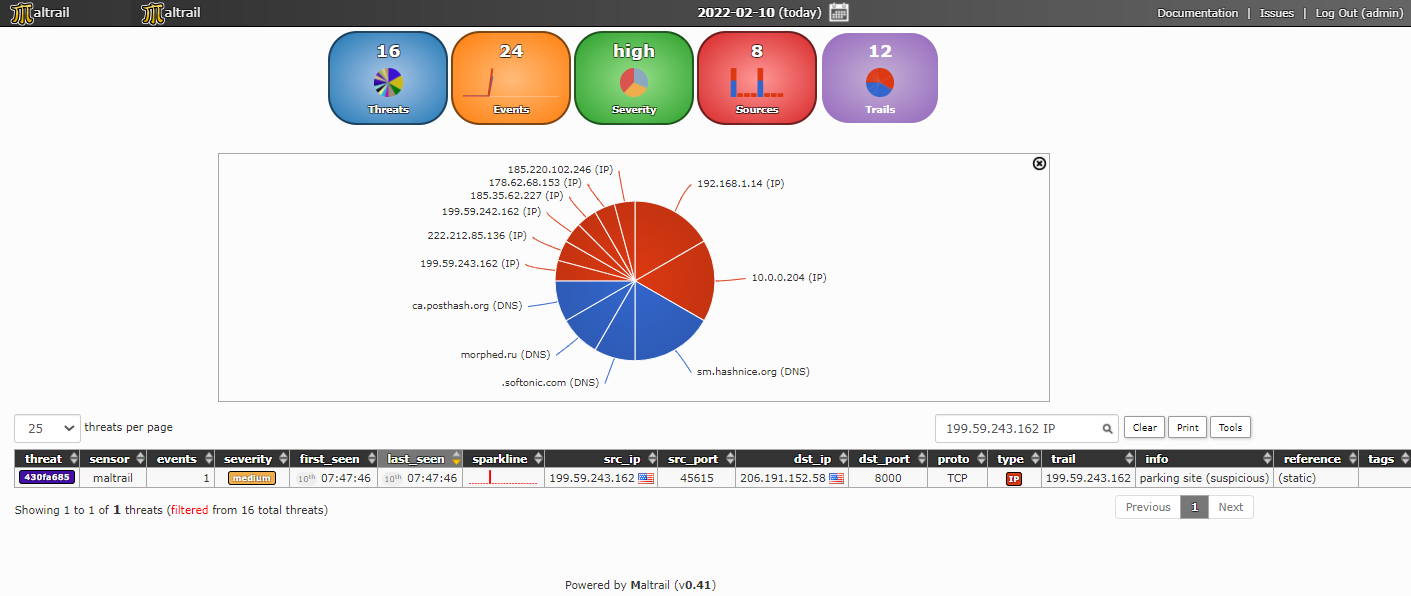
**Figura 27.** Gráfico de números de eventos

**Threats** El cuadro representa el porcentaje de las principales amenazas en forma de gráfico circular (Nota: el área gris contiene todas las amenazas con <1 % en eventos totales cada una), con el número total de amenazas en la parte superior.



**Figura 28.** Gráfico de las principales amenazas

**Trails** El cuadro representa el porcentaje de los principales ataques provenientes del exterior en forma de gráfico circular, con el número total de accesos en la parte superior. Cada uno de esos cuadros está activo, por lo tanto, al hacer clic en uno de ellos, se obtendrá un gráfico más detallado.



**Figura 29.** Grafico ataques provenientes del exterior

* EVENTOS REGISTRADOS EN FORMA DE TABLA

La parte inferior contiene una representación en forma de tabla paginada la cual contiene todos los eventos. Cada entrada contiene los detalles para las amenazas registradas de forma individual:



**Figura 30.** Representación en forma de tabla

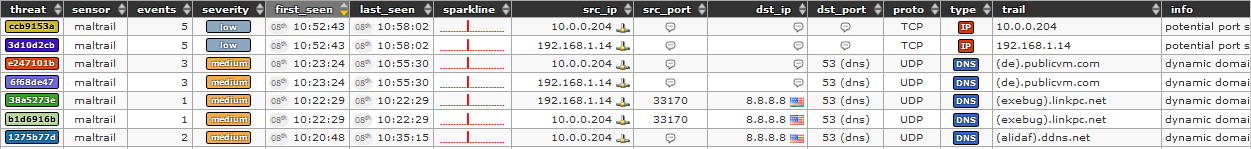
* **threat** contiene la identificación única de la amenaza.
* **sensor** contiene los nombres de los sensores en los que se ha activado el evento.
* **events** contiene el número total de eventos para una amenaza actual.
* **severity** contiene la gravedad evaluada de amenaza.
* **first\_seen** retiene la hora del primer evento.
* **last\_seen** retiene la hora del último evento.
* **sparkline** contiene un pequeño gráfico brillante que representa la actividad de la amenaza.
* **src\_ip** contiene las direcciones IP de origen de una amenaza.
* **src\_port** contiene los puertos de origen.
* **proto** contiene protocolo(s).
* **info** contiene más información sobre la amenaza/rastro.
* **reference** contiene una fuente de la entrada en la lista negra.
* **tags** contiene etiquetas definidas por el usuario para una ruta determinada.

# ANEXO 4

# ANÁLISIS REALIZADOS CON LA HERRAMIENTA MALTRAIL

* DETALLES DE LA AMENAZA

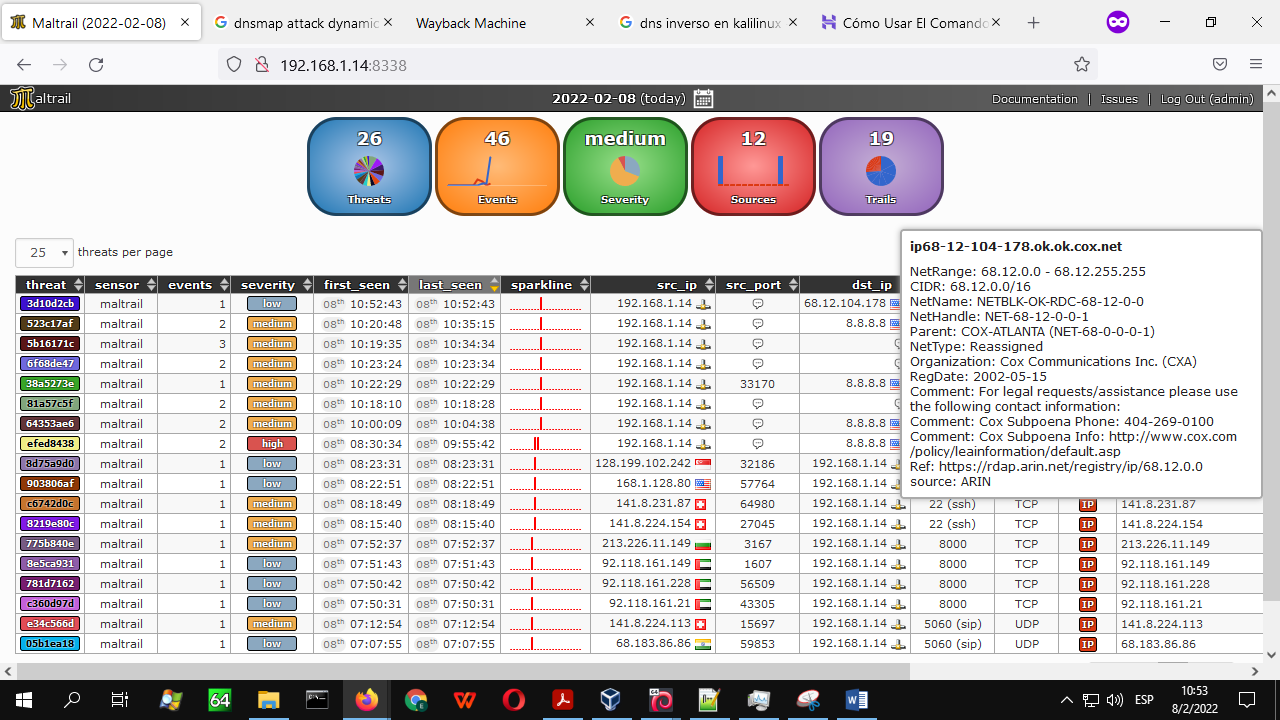
Se proporcionarán los detalles de la amenaza, incluidos los detalles de su origen y destino, junto con el destino y los puertos de origen. Esto también tendrá la cantidad de paquetes filtrados y marcados como amenazas.



**Figura 31.** Detalle de las amenazas

* BÚSQUEDA DE DNS INVERSA

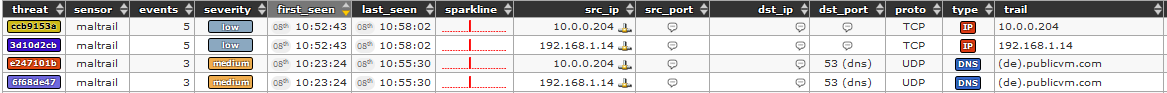
La búsqueda de DNS se realiza con la IP para verificar su gravedad y sus detalles, como cuándo y dónde está alojado, en qué lugar y a qué hora, esto será útil para bloquear todo el contenido del servidor web específico.



**Figura 32.** Búsqueda inversa de DNS

* DETECCIÓN DE ESCANEOS MASIVOS

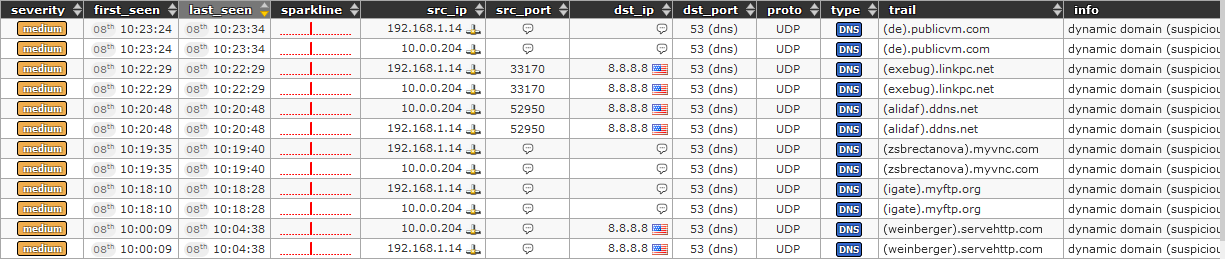
Los escaneos masivos se detectarán en la red en función de las IP conocidas basadas en la web. Para que el administrador pueda revisar la informacion generada, lo cual permite evitar posibles daños causados por los atacantes, para poder tomar decisiones necesarias.



**Figura 33.** Detección de escaneos masivos

* ESCANEO DE DOMINIO DINÁMICO

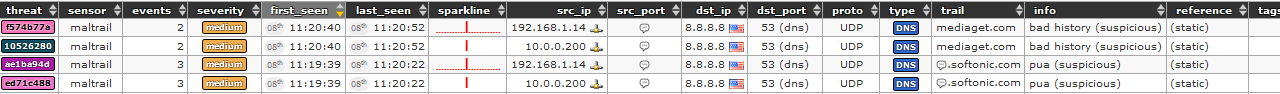
Los sitios web que tendrán las IP dinámicas para acceder a los nodos de salida de la red como se muestra en la tabla seccion info alerta de (dynamic domain).



**Figura 34.** Escaneo de dominio dinámico

* FILTRADO DE DESCARGAS DIRECTAS DE ARCHIVOS

Los sitios adquirirán una opción conocida como descargas con un solo clic que puede resultar en el archivo malicioso que da como resultado comprometer el objetivo en muy poco tiempo, esto debe evitarse utilizando este filtro.



**Figura 35.** Filtrado de descarga directa

* TABLERO DE INFORME PARA EL CLIENTE

En la tabla de informe se mostrara a detalle el análisis realizado al tráfico mediante el filtrado de la gravedad y la cantidad de amenazas que se presentan frente al usuario con el inicio de sesión realizado.



**Figura 36.** Tabla de análisis