UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"Monitor de Seguridad de Red Zeek Open Source como mecanismo de seguridad empresarial en entornos libres, 2023"

Tesis para optar el título profesional de:
INGENIERO DE SISTEMAS

Presentado por:
Bach. Amorhin Rojas Huarhuachi

Asesor:
Ing. Hubner Janampa Patilla

Ayacucho - Perú
2023

DEDICATORIA

A mis seres queridos por el apoyo que me brindan en todo momento. A los maestros de la Escuela Profesional de Ingeniería de Sistemas, por incluirme su conocimiento durante desarrollo de mi carrera, agradecido con el asesor de tesis quien me ha guiado con sus conocimientos, y a mis amigos por el apoyo y motivación.

AGRADECIMIENTO

En primer lugar, a Dios, por permitirme llegar a este punto en mi vida. Asimismo, a mis padres Victor y Cicilia y mis hermanos, Hilda, Luzmila, Deter, Nelida, Elvis y Ana Belinda por el apoyo incondicional que me han permitido lograr de mis metas.

A mis tíos Melchor y Victoria, mi primo Jack que siempre me han prestado un gran apoyo personal.

A la Universidad Nacional de San Cristóbal de Huamanga, en especial a la Escuela Profesional de Ingeniería de Sistemas en la que me formé.

A mi asesor, el Dr. Ing. Hubner Janampa Patilla por la ayuda en la elaboración de esta tesis.

A todos mis seres queridos, y a los que me faltó nombrar, les digo gracias por el apoyo que me brindaron.

RESUMEN

Este proyecto de investigación tiene como objetivo principal analizar cómo el monitor de seguridad de red Zeek Open Source se convierte en un mecanismo efectivo de seguridad empresarial en entornos libres en el año 2023. Se abordarán tres aspectos clave de Zeek: los controladores de eventos de red, los intérpretes de políticas de script y los motores de eventos, para demostrar su relevancia y utilidad en el ámbito empresarial.

En primer lugar, se explorará cómo el monitor de seguridad de red Zeek basado en controladores de eventos de red desempeña un papel fundamental en la detección y análisis de actividades maliciosas en la red empresarial. Se examinarán las capacidades de captura de datos, extracción de información y generación de alertas que ofrecen estos controladores, brindando una visión integral de las amenazas de seguridad presentes en el entorno empresarial.

En segundo lugar, se investigará el enfoque basado en intérpretes de políticas de script de Zeek que se traduce en una capacidad flexible y personalizable para establecer políticas de seguridad específicas de la empresa.

Por último, se estudiará el uso de motores de eventos en Zeek. Estos motores permiten el análisis en tiempo real de los eventos de red, la correlación de datos y la generación de informes, fortaleciendo así la capacidad de Zeek como mecanismo de seguridad empresarial.

En resumen, este proyecto busca implementar y evaluar el monitor de seguridad de red Zeek Open Source como un mecanismo confiable de seguridad empresarial en entornos libres en el año 2023. Se enfocará en los controladores de eventos de red, los intérpretes de políticas de script y los motores de eventos para demostrar su importancia y su capacidad para detectar, analizar y responder a las amenazas de seguridad en el entorno empresarial.

Palabras claves: Zeek Open Source, seguridad, ataques informáticos, monitoreo de seguridad de red, NSM.

ABSTRACT

The main objective of this research project is to analyze how the Zeek Open Source network security monitor becomes an effective enterprise security mechanism in free environments in the year 2023. Three key aspects of Zeek - network event handlers, script policy interpreters and event engines - will be addressed to demonstrate their relevance and usefulness in the enterprise environment.

Firstly, it will explore how the Zeek network security monitor based on network event handlers plays a key role in detecting and analyzing malicious activity in the enterprise network. It will examine the data capture, information extraction and alert generation capabilities offered by these controllers, providing a holistic view of the security threats present in the enterprise environment.

Secondly, Zeek's scripted policy interpreter-based approach will be investigated, resulting in a flexible and customisable ability to establish enterprise-specific security policies.

Finally, the use of event engines in Zeek will be explored. These engines enable real-time analysis of network events, data correlation and report generation, thus strengthening Zeek's capability as an enterprise security mechanism.

In summary, this project aims to implement and evaluate the Zeek Open Source network security monitor as a reliable enterprise security mechanism in free environments by 2023. It will focus on network event handlers, script policy interpreters and event engines to demonstrate their importance and their ability to detect, analyze and respond to security threats in the enterprise environment.

Keywords: Zeek Open Source, security, computer attacks, network security monitoring, NSM.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

En el actual panorama empresarial, la seguridad de la información se ha convertido en un aspecto crucial para las organizaciones, especialmente en un entorno cada vez más conectado y dependiente de las redes. La protección de los activos y la privacidad de los datos se han vuelto prioridades estratégicas para salvaguardar la continuidad del negocio y mantener la confianza de los clientes.

En este contexto, surge la necesidad de implementar mecanismos de seguridad eficientes que permitan detectar y prevenir posibles amenazas en las redes empresariales. Uno de estos mecanismos es el monitor de seguridad de red Zeek Open Source, una herramienta de código abierto diseñada para analizar y monitorear el tráfico de red con el fin de identificar comportamientos sospechosos y posibles intrusiones.

El presente trabajo de investigación tiene como objetivo explorar cómo el monitor de seguridad de red Zeek Open Source puede ser utilizado como un mecanismo de seguridad empresarial en entornos libres en el año 2023. Para lograr este objetivo, se realizará un estudio aplicado de nivel descriptivo, con un enfoque en el diseño no experimental.

Los problemas secundarios a abordar se centran en comprender cómo el monitor de seguridad de red Zeek Open Source, basado en controladores de eventos de red, intérpretes de políticas de script y motores de eventos, puede contribuir como mecanismo de seguridad empresarial en entornos libres. Estos componentes fundamentales de Zeek Open Source permiten la detección temprana de amenazas, el análisis en tiempo real y la generación de alertas, brindando así una capa adicional de protección a las redes empresariales.

A través de la implementación de Zeek Open Source, se busca fortalecer la seguridad empresarial y proporcionar a las organizaciones una mayor visibilidad y control sobre su infraestructura de red. Al utilizar esta herramienta de código abierto, las empresas pueden aprovechar la comunidad de desarrolladores y expertos en seguridad, beneficiándose de las actualizaciones y mejoras constantes que promueve el enfoque colaborativo.

En resumen, este trabajo de investigación tiene como propósito implementar el monitor de seguridad de red Zeek Open Source como mecanismo de seguridad empresarial en entornos libres en el año 2023. A través de la exploración de sus componentes clave y su potencial en la detección de amenazas, se busca proporcionar a las organizaciones una solución efectiva y de bajo costo para proteger sus activos y salvaguardar su información sensible.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. DIAGNÓSTICO Y ENUNCIADO DEL PROBLEMA

El aumento significativo de los ciberataques en el contexto post-pandémico del COVID-19 ha generado una creciente preocupación en las empresas. En este contexto, se ha identificado la necesidad de implementar mecanismos de seguridad eficaces que protejan la red empresarial. Sin embargo, en entornos libres y de código abierto, es importante encontrar soluciones de seguridad accesibles y confiables. En este sentido, el monitor de seguridad de red Zeek Open Source surge como una posible alternativa en vista que está diseñado para analizar y detectar actividades maliciosas en la red. Se basa en controladores de eventos de red, intérpretes de políticas de script y motores de eventos para recopilar y analizar datos de tráfico de red en tiempo real, además de ser gratuito.

Con el objetivo de evaluar la viabilidad y efectividad del monitor de seguridad de red Zeek Open Source como mecanismo de seguridad empresarial en entornos libres, se plantea la presente investigación. A través de un enfoque descriptivo y un diseño no experimental, se busca implementar esta herramienta y analizar su desempeño basado en controladores de eventos de red, intérpretes de políticas de script y motores de eventos. Los resultados de esta investigación proporcionarán información valiosa para las organizaciones interesadas en utilizar Zeek como parte de su estrategia de seguridad en redes empresariales libres.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general

¿Cómo el monitor de seguridad de red Zeek Open Source es un mecanismo de seguridad empresarial en entornos libres, 2023?

1.2.2. Problemas específicos

a. ¿Cómo el monitor de seguridad de red Zeek Open Source basado en controladores de eventos de red es un mecanismo de seguridad empresarial en entornos libres, 2023?
b. ¿Cómo el monitor de seguridad de red Zeek Open Source basado en intérpretes de políticas de script es un mecanismo de seguridad empresarial en entornos libres, 2023?

c. ¿Cómo el monitor de seguridad de red Zeek Open Source basado en motores de eventos es un mecanismo de seguridad empresarial en entornos libres, 2023?

1.3. OBJETIVOS

1.3.1. Objetivo general

Implementar el monitor de seguridad de red Zeek Open Source como mecanismo de seguridad empresarial en entornos libres, 2023.

1.3.2. Objetivos específicos

a. Implementar el monitor de seguridad de red Zeek Open Source basado en controladores de eventos de red como mecanismo de seguridad empresarial en entornos libres, 2023.
b. Implementar el monitor de seguridad de red Zeek Open Source basado en intérpretes de políticas de script como mecanismo de seguridad empresarial en entornos libres, 2023.
c. Implementar el monitor de seguridad de red Zeek Open Source basado en motores de eventos como mecanismo de seguridad empresarial en entornos libres, 2023.

1.4. HIPÓTESIS DE LA INVESTIGACIÓN

“Las investigaciones de tipo descriptivo no requieren formular hipótesis; es suficiente plantear algunas preguntas de investigación que, como ya se anotó, surgen del planteamiento del problema, de los objetivos y, por supuesto, del marco teórico que soporta el estudio” (Bernal, 2010, p. 136).

La investigación que se desarrollará es descriptiva, por lo que se optó por no plantear hipótesis.

CAPÍTULO II
MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

En diferentes investigaciones relacionadas con el monitoreo y control de redes, se ha demostrado el impacto positivo de herramientas de código abierto y software libre en entornos empresariales.

Por ejemplo, Quispe (2018) en su tesis titulada "Implementación de un Sistema de Monitoreo y Control de Red para un Canal de Televisión, Basado en Herramientas OPEN SOURCE y Software Libre" de la Universidad Nacional del Antiplano, concluyó que la implementación del sistema de monitoreo utilizando la herramienta NAGIOS y plugins en CENTOS permitió un aumento significativo en la supervisión de equipos y servicios críticos para los encargados de red del canal WILLAX Televisión.

En otro trabajo de investigación, Zambrano et al. (2019) desarrollaron un "Sistema de Monitoreo de Infraestructura para la Gestión de Recursos de TI en la Empresa COGA". Mediante el módulo Network Performance Monitor (NPM), se pudo determinar que algunos equipos de infraestructura estaban próximos a alcanzar su límite de consumo, y el estado de su disponibilidad se presentaba a través de reportes, alertas y presentaciones gráficas en tiempo real. Además, el módulo Solarwinds Netflow Traffic Analyzer (NTA) permitió identificar el consumo de ancho de banda y proporcionar reportes detallados para mejorar el rendimiento.

Álvarez (2015) en su investigación titulada "Análisis, Diseño e Implementación de una herramienta de Monitoreo y Control de Datacenter Basado en Herramientas OPEN SOURCE aplicado al Banco de Guayaquil" de la Universidad Politécnica Salesiana Sede Guayaquil, se construyó un software de código abierto capaz de monitorear dispositivos, enlaces y servicios en el datacenter del Banco de Guayaquil. Este sistema permitió el monitoreo de los parámetros SLA, incluyendo tiempos de respuesta y rendimiento en términos de CPU, memoria y consumo de red.

Álvarez (2019) en su investigación de Master en Seguridad de las Tecnologías de la Información y las Comunicaciones, titulada "Despliegue de la herramienta Zeek y su posterior explotación para el análisis de actividades sospechosas en la red", se concluyó que Zeek proporciona herramientas de monitoreo y detección de comportamientos anómalos, lo que permite identificar infecciones o amenazas latentes. Además, el uso de herramientas de software libre en entornos

empresariales brinda una visibilidad valiosa para aplicar controles de seguridad al tráfico de red entrante, saliente y circulante.

En resumen, estas investigaciones destacan el valor de las herramientas de código abierto y software libre, como Zeek Open Source, en el monitoreo de redes empresariales, brindando una mayor visibilidad y detección de amenazas potenciales.

2.2. MARCO TEÓRICO

2.2.1. Zeek Open Source

Según la documentación oficial, Zeek es una herramienta de análisis de tráfico de red de código abierto que opera de manera pasiva. Su funcionalidad principal es actuar como un sistema de monitorización de seguridad de red (NSM), brindando soporte en la detección e investigación de actividades sospechosas o maliciosas.

2.2.1.1. Características

Las características que hacen a Zeek Open Source una herramienta valiosa para la monitorización de la seguridad de la red son:

- Plataforma de seguridad de red de código abierto que se centra en la captura y análisis de tráfico de red en tiempo real para detectar amenazas. (Duchene, 2020)
- Es un enfoque basado en eventos para la monitorización de red y la seguridad que proporciona una visibilidad completa de la actividad de la red. (Barr, 2020)
- Cuenta con un lenguaje de scripting poderoso y flexible que permite a los usuarios personalizar su funcionamiento y ampliar sus capacidades de análisis. (Kopp, 2020)
- Es capaz de realizar análisis sofisticados de la actividad de la red, incluyendo la identificación de patrones de comportamiento, la detección de malware y la reconstrucción de sesiones de red completas. (Corelight, 2021)
- Además, según su documentación oficial, es altamente escalable y se puede utilizar para monitorear redes de cualquier tamaño, desde pequeñas empresas hasta grandes organizaciones gubernamentales y de investigación.

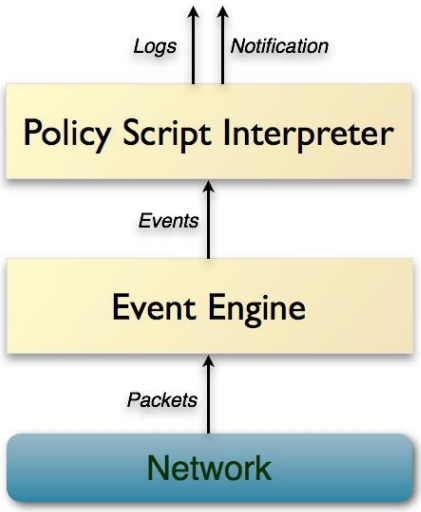
2.2.1.2. Arquitectura y componentes

De acuerdo a Singh & Khanuja (2021), Zeek consta de varios componentes clave, como un filtro de paquetes, que captura y decodifica el tráfico de red, un lenguaje de scripts, que se utiliza para

definir reglas de análisis personalizadas aparte de las que vienen por defecto, y un marco de registro, que registra los datos en disco para su posterior análisis.

Figura 1

Arquitectura de Zeek



Nota. Adaptado de *Architecture*, de The Zeek Project, Zeek Documentation (https://docs.zeek.org/en/master/about.html).

2.2.1.3. Principales protocolos de red admitidos por Zeek Open Source

Uno de los puntos fuertes de Zeek Open Source es la amplia capacidad para analizar y procesar diversos protocolos de red. Bejtlich (2020) menciona que esta herramienta puede identificar estos protocolos incluso si se están ejecutando en puertos no estándar, utilizando una función llamada Detección Dinámica de Protocolos (DPD).

IP (Internet Protocol). Zeek analiza y registra información relacionada con el protocolo IP, como direcciones IP de origen y destino, encabezados IP, y otras características relevantes.

TCP (Transmission Control Protocol). Zeek monitorea y analiza el tráfico TCP, capturando y registrando información sobre las conexiones TCP establecidas, los puertos utilizados y otros detalles relacionados con el protocolo.

UDP (User Datagram Protocol). Zeek Open Source examina el tráfico UDP y registra los puertos de origen y destino, proporcionando información sobre los flujos de datos UDP.

ICMP (Internet Control Message Protocol). Zeek Open Source analiza y registra mensajes ICMP, lo que permite el monitoreo y detección de actividades relacionadas con este protocolo, como los mensajes de eco (ping).

HTTP (Hypertext Transfer Protocol). Zeek descompone y analiza el tráfico HTTP capturando así información detallada sobre las solicitudes y respuestas HTTP, los encabezados, las URL's y otros aspectos relacionados.

SMTP (Simple Mail Transfer Protocol). Zeek analiza el tráfico SMTP, capturando y registrando información relevante sobre los correos electrónicos enviados y recibidos, los remitentes, los destinatarios y otros atributos asociados.

DNS (Domain Name System). Zeek Open Source analiza el tráfico DNS para extraer información sobre consultas y respuestas DNS, como nombres de dominio, direcciones IP asociadas, registros de recursos y otros.

FTP (File Transfer Protocol). Zeek Open Source analiza el tráfico FTP, capturando y registrando información sobre las conexiones FTP, las transferencias de archivos, los comandos y respuestas FTP, y otros detalles relevantes. Esto permite la supervisión y el análisis de actividades de transferencia de archivos a través del protocolo FTP.

SSH (Secure Shell). Zeek detecta y registra conexiones SSH establecidas en la red. Esto incluye información sobre los inicios de sesión, la autenticación, las claves públicas y otros aspectos relacionados con SSH. Gracias a lo cual se puede monitorear y detectar conexiones SSH tanto legítimas como potencialmente maliciosas.

SSL/TLS (Secure Sockets Layer/Transport Layer Security). Zeek analiza el tráfico SSL/TLS para identificar y extraer información relacionada con las sesiones de cifrado seguro. Esto incluye certificados, cifrado utilizado, versiones del protocolo, negociación de claves y otros detalles relevantes, todo ello para detectar comportamientos sospechosos o inseguros relacionados con SSL/TLS.

SIP (Session Initiation Protocol). Zeek Open Source analiza y registra el tráfico SIP, permitiendo el monitoreo y la extracción de información relacionada con las sesiones de comunicación en tiempo real, como llamadas de voz y vídeo.

DHCP (Dynamic Host Configuration Protocol). Zeek Open Source analiza el tráfico DHCP para obtener información sobre la asignación de direcciones IP, arrendamiento de direcciones, solicitudes y respuestas DHCP, y otra información relevante para la configuración dinámica de hosts en una red.

NTP (Network Time Protocol). Zeek analiza y registra el tráfico NTP, permitiendo el monitoreo y la sincronización de la hora en una red, capturando información sobre las consultas y respuestas NTP, incluyendo detalles como las fuentes de tiempo, las versiones del protocolo y los ajustes de sincronización. Esta capacidad ayuda a mantener la precisión y consistencia en la sincronización de tiempo en la red.

SNMP (Simple Network Management Protocol). Zeek analiza y registra el tráfico SNMP, lo que permite el monitoreo y la gestión de dispositivos de red. Los datos capturados pueden ser identificadores de objetos, valores de los objetos y los mensajes de error. Esto facilita el seguimiento y la supervisión de la infraestructura de red mediante la obtención de información sobre el rendimiento y el estado de los dispositivos SNMP habilitados.

IRC (Internet Relay Chat). Zeek Open Source analiza y registra el tráfico IRC, monitoreando y supervisando las conversaciones en los canales de chat. La información de los mensajes enviados, recibidos, usuarios involucrados y otros detalles relacionados con las interacciones en el chat son capturados.

Por defecto, cuando Zeek ve tráfico de red usando un protocolo que conoce, registrará los detalles de esas transacciones en un archivo. Por supuesto, el registro es totalmente personalizable, pero mientras Zeek analiza y decodifica el protocolo, le ofrece un mecanismo para crear una lógica personalizada para procesar las transacciones en el tráfico que está examinando. Trata las acciones tomadas por un protocolo como una serie de eventos, para los que se pueden registrar manejadores de eventos escritos en código Zeek.

2.2.1.4. Monitoreo con Zeek

Detección y flujo de respuesta. Según la documentación oficial, incluso con las configuraciones iniciales, esta herramienta ofrece datos de transacciones y datos de contenido extraído, en forma de registros que resumen los protocolos y archivos vistos.

Zeek puede ser utilizado dentro de un flujo de trabajo de *alerta de detección de incidentes*. En este escenario, un IDS crea una alerta que podría no ser detallada, con la que los analistas o miembros del equipo de seguridad tienen la posibilidad de "pivotar" desde la alerta IDS a una variedad de registros generados por Zeek. Si la alerta IDS proporciona la identificación de comunidad (community ID) admitida por Zeek, el analista puede relacionar fácilmente la alerta IDS con registros específicos con lo cual se puede resolver el incidente. Como mínimo, el analista puede acelerar el proceso de validación y verificación de la alerta al tener acceso a datos más allá de la notificación IDS inicial.

Instrumentación y recolección. La mayoría de usuarios utilizan Zeek para obtener información casi en tiempo real sobre los patrones de uso de la red.

Esta herramienta se puede ejecutar en un único ordenador utilizado para fines informáticos generales, vigilando el tráfico de red hacia y desde ese único ordenador o en uno seleccionado exclusivamente, llamado sensor, para la supervisión de la seguridad. Este sensor es ubicado en un entorno que ofrece visibilidad a varios ordenadores para instrumentar ese segmento de red.

Almacenamiento y revisión. A medida que Zeek monitoriza o procesa el tráfico de una red, crea una variedad de registros y otros artefactos, además de realizar determinados procesos de gestión de registros, como la compresión y el archivado.

Los métodos de revisión pueden incluir el uso de herramientas de procesamiento de texto empaquetadas con el sistema operativo subyacente. Dependiendo del formato de los registros, los usuarios pueden aplicar herramientas de procesamiento más especializadas, algunas de las cuales están disponibles con Zeek. En muchos casos, los administradores de Zeek envían los registros a aplicaciones especializadas de almacenamiento y revisión. Estas suelen denominarse colectivamente plataformas de gestión de eventos de seguridad e información (SIEM). Algunas de estas plataformas de gestión de registros y SIEM están disponibles como ofertas de código abierto, mientras que otras están disponibles comercialmente.

2.2.1.5. Beneficios de la monitorización con Zeek

Los autores Li et al. (2019), concluyeron en su trabajo de investigación que los beneficios de la monitorización de la red son los siguientes:

- Detección temprana de posibles amenazas y vulnerabilidades en la red, lo que permite tomar medidas preventivas para evitar incidentes de seguridad.
- Identificación de patrones de tráfico y comportamiento anómalo en la red, lo que ayuda a detectar posibles intentos de ataques o intrusiones.
- Mejora de la capacidad de respuesta ante incidentes de seguridad, al permitir una identificación rápida y precisa de la fuente del problema.
- Reducción del tiempo de inactividad y mejora de la disponibilidad de los servicios en la red, ya que la monitorización permite detectar y solucionar problemas de manera oportuna.
- Mejora de la toma de decisiones en cuanto a inversiones y mejoras en la infraestructura de seguridad, ya que se pueden identificar áreas críticas y realizar ajustes en consecuencia.

A lo que Ahmed & Hassan (2021) añaden:

- Cumplimiento normativo y regulatorio: La monitorización de la seguridad de la red ayuda a las organizaciones a cumplir con los requisitos normativos y regulatorios en materia de seguridad de la información. Esto incluye la identificación y el seguimiento de las políticas de seguridad, la generación de informes de cumplimiento y la demostración de buenas prácticas de seguridad.

2.2.2. Seguridad empresarial

De acuerdo a Woody (2013), asegurar la empresa, de forma conceptual, puede parecer una afirmación binaria o una idea universalmente entendida. Nos han enseñado a pensar que, si tomamos ciertas medidas, como desarrollar procesos seguros, impartir formación en seguridad e implantar tecnologías de seguridad, habremos asegurado la empresa. La seguridad no es binaria y su aplicación debe ser flexible y ágil basada en el riesgo para los datos de la empresa.

Por ende, el enfoque de seguridad empresarial debe ir más allá de la simple mitigación de amenazas.

2.2.2.1. Obstáculos de la seguridad empresarial

Deficiencias de la arquitectura de seguridad actual. La arquitectura de seguridad actual no responde a las tendencias actuales de la empresa, como las iniciativas "traiga

su propio dispositivo" (BYOD) y la nube; tampoco aborda las comunicaciones internas en las que no suelen ser obligatorios los controles de seguridad, pero es donde suelen estar los sistemas y datos más sensibles y críticos de una empresa.

Comunicar la seguridad de la información. A menudo, los profesionales de la seguridad se centran tanto en la responsabilidad de proteger la empresa que pierden de vista el objetivo comercial. Esto conduce al perjuicio del éxito del equipo de seguridad en general e influye negativamente en las decisiones de diseño y compra.

Dado que la seguridad no es una función de TI común y, generalmente, incomprendida, puede ser difícil conseguir que la alta dirección y otros equipos de TI la acepten.

A menudo, la seguridad es una idea tardía y, por tanto, no es bien recibida. Cabe señalar que todos los empleados de la empresa son responsables de la seguridad y deben adoptar la integración de la seguridad en todos los procesos informáticos y empresariales aplicables. La seguridad de una empresa es tan buena como su eslabón más débil.

El coste de la seguridad de la información. La dificultad para proporcionar datos cuantificables que respalden el coste y la solicitud de compras relacionadas con la seguridad es significativa, la razón general de que esto sea así se debe a la fallida arquitectura de seguridad de antaño en la que se sigue intentando meter todo con calzador.

El mensaje contradictorio de la seguridad empresarial. Existen facciones dentro de la seguridad que dicen "haz esto, no hagas aquello", mientras que otros dicen lo contrario. Esto lleva a que los equipos de personal de seguridad tengan ideas y puntos de vista muy diferentes sobre cómo implementar la seguridad para la empresa, determinar el riesgo y gestionar las operaciones de seguridad cotidianas.

Demostrar un negativo. Uno de los retos más importantes de la seguridad de la información es probar un negativo. Se trata, por ejemplo, de decir que, si se adoptan medidas o acciones específicas o se adquiere una tecnología concreta, se impiden las intrusiones exitosas en la red. Esto se debe en parte a que no existe una tecnología

desplegada que nos proporcione esta información y en parte a que sólo nos enteramos de una pequeña parte de las violaciones.

2.2.2.2. Monitoreo de seguridad

Estrategias de monitoreo. Para saber qué ocurre en los sistemas, en la red y quién accede a los datos, deben emplearse estrategias de supervisión para detectar y mitigar comportamientos maliciosos y no intencionados.

No sólo es necesario disponer de herramientas de supervisión, sino también de conocimientos especializados para interpretar los resultados e identificar patrones en los mismos, ya sea manualmente o mediante una capacidad automatizada.

A continuación, en la Tabla 3, se resumirá las distintas estrategias de monitoreo que presenta Woody (2013).

Tabla 1

Estrategias de monitoreo

Estrategia	Reseña
Supervisión basada en modelos de confianza	Los modelos de confianza son el fundamento recomendado para la supervisión de la seguridad empresarial. La seguridad y la supervisión centradas en los datos son las más eficaces, ya que son específicas de los datos presentes y son tan transitorias como los propios datos. A continuación, se mencionan los puntos de supervisión dentro del modelo de confianza que justifican una mayor discusión para supervisar eficazmente. ● Monitoreo de datos ● Monitoreo de procesos ● Monitoreo de aplicaciones ● Monitoreo de usuarios

Supervisión basada en el límite de la red	Es una táctica básica de defensa en profundidad para mitigar las amenazas más comunes observadas desde segmentos de red de baja a alta seguridad. El límite más común es el borde de Internet de la empresa, sin embargo, existen otros límites de red que pueden requerir supervisión, como las conexiones de socios comerciales, filiales, redes privadas virtuales (VPN) y proveedores de servicios. Lo ideal es crear etiquetas para los tipos de límites definidos por la empresa y asignar los requisitos de supervisión en consecuencia.
Supervisión basada en el segmento de red	Hay segmentos de red que tienen un valor más alto basado en la criticidad para el negocio. Estos segmentos pueden requerir una supervisión adicional no sólo para cumplir la normativa u otros requisitos, sino también para garantizar que los administradores, los propietarios y la seguridad de TI sepan lo que ocurre en un segmento concreto de la red. Los segmentos deben documentarse según su finalidad, como RRHH, PCI, correo electrónico, etc., con todas las indicaciones de denominación, controles y supervisión. Este método sólo es eficaz si la red tiene una demarcación clara de los segmentos de red en los que la supervisión puede situarse estratégicamente en la red y controlarse.

Monitoreo de seguridad de red. Bejtlich (2020), menciona que el monitoreo de seguridad (NSM) es la recopilación, el análisis y la escalada de indicaciones y advertencias para detectar y responder a intrusiones antes de que ocurra un daño a nivel empresarial u organizacional.

Añade también que la NSM no es la única respuesta al problema de detectar, responder y contener a los intrusos, ni quizás la más completa, pero es una de las mejores formas de pasar de cero defensas a cierta capacidad defensiva y frustrar la misión de los posibles intrusos.

Existen tres fases en el ciclo de monitoreo de seguridad de red, de acuerdo a Sanders & Smith (2013), las cuales son: colección, detección y análisis.

Tabla 2

Fases del ciclo NSM

Fase	Reseña
Recolección o recopilación	Se produce con una combinación de hardware y software que se utilizan para generar, organizar y almacenar datos para la detección y el análisis de NSM. Las categorías más comunes de datos NSM incluyen Datos de Contenido Completo, Datos de Sesión, Datos Estadísticos, Datos de Cadena de Paquetes y Datos de Alerta. Dependiendo de las necesidades de la organización, la arquitectura de la red y los recursos disponibles, estos tipos de datos pueden ser utilizados principalmente para la detección, para el análisis, o para ambos. La recopilación incluye tareas como: ● Definir dónde existe la mayor cantidad de riesgo en la organización. ● Identificar las amenazas a los objetivos de la organización. ● Identificar las fuentes de datos relevantes. ● Refinamiento de las porciones de recolección de fuentes de datos.

	● Configuración de puertos SPAN para recopilar datos de paquetes. ● Creación de almacenamiento SAN para la retención de registros. ● Configuración de hardware y software de recopilación de datos.
Detección	Es el proceso mediante el cual se examinan los datos recopilados y se generan alertas basadas en eventos observados y datos inesperados. Esto suele hacerse mediante algún tipo de detección basada en firmas, anomalías o estadísticas. El resultado es la generación de datos de alerta. Aunque la mayor parte de la detección se realiza mediante software, parte de la detección se realiza mediante análisis manual de las fuentes de datos. Este es especialmente el caso del análisis retrospectivo.
Análisis	Es la etapa final del ciclo NSM y la que más tiempo consume. Se produce cuando un humano interpreta e investiga los datos de la alerta. Esto a menudo implica la recopilación de datos de otras fuentes. Esta etapa puede incluir tareas como: ● Análisis de paquetes ● Análisis forense de redes ● Análisis forense de host ● Análisis de malware.

El bucle del ciclo NSM se cierra tomando las lecciones aprendidas de la fase de detección y análisis de cualquier anomalía y dando forma a la estrategia de recopilación de la organización.

Gama de datos del NPM.

- Datos de contenido completo: Se refiere a toda la información que pasa a través de una red. No se filtran los datos para recopilar únicamente información asociada a alertas de seguridad ni se guardan registros de aplicaciones. Son copias exactas del tráfico tal y como se ve en la red.
- Datos de contenido extraído: Son los flujos de datos de alto nivel, como archivos, imágenes y medios, transferidos entre ordenadores. A diferencia de los datos de contenido completo, que incluyen cabeceras de los niveles inferiores del proceso de comunicación, con el contenido extraído no nos preocupamos de las direcciones MAC, direcciones IP, protocolos IP, etcétera. En su lugar, si dos ordenadores intercambian un archivo, revisamos el archivo. Si un servidor web transfiere una página web a un navegador, revisamos la página web. Y, si un intruso transmite una pieza de malware o un gusano, revisamos el malware o el gusano.
- Datos de sesión: Son un registro de la conversación entre dos nodos de red. Estos datos resumen muchos de los detalles en elementos básicos, incluyendo la marca de tiempo, la dirección IP de origen, el puerto de origen, la dirección IP de destino, el puerto de destino, el protocolo, los bytes de aplicación enviados por el origen y destino, entre otros. Se podrían generar datos de sesión a partir de los datos de contenido completo, pero si el espacio en el disco duro es escaso, registrar sólo los datos de sesión podría ser una buena opción.
- Datos de transacción: Son similares a los datos de sesión, excepto que se centran en entender las peticiones y respuestas intercambiadas entre dos dispositivos de red. No es tan detallada como los datos de contenido completo, pero tampoco tan abstracta como los datos de sesión.
- Datos estadísticos: Describen el tráfico resultante de varios aspectos de una actividad.
- Metadatos: Son *datos sobre datos*. Para generarlos se extraen elementos clave de la actividad de la red y, a continuación, se utiliza alguna herramienta externa para comprenderlos.

- Datos de alerta: Reflejan si el tráfico activa una alerta en una herramienta NSM. Se basan en patrones de bytes o recuentos de actividad, o incluso en opciones más complicadas que analizan en profundidad los paquetes. Una fuente de este tipo de datos es un sistema de detección de intrusos (IDS).

2.2.2.3. Riesgos y amenazas que enfrentan las empresas

Amenazas internas. Son aquellas que provienen de empleados o personal interno de la organización y pueden incluir acciones maliciosas, negligencia o errores no intencionales. Estas amenazas pueden comprometer la seguridad de los activos de información de la empresa (Jøsang, Ismail, & Boyd, 2007).

Ataques de malware. El malware, como virus, gusanos y troyanos, representa una amenaza significativa para las empresas. Estos programas maliciosos pueden infiltrarse en los sistemas de la empresa, robar información confidencial o dañar los sistemas operativos y la infraestructura (Kumar & Chang, 2019).

Ataques de phishing. Los ataques de phishing son intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas o datos financieros. Los delincuentes se hacen pasar por entidades legítimas en correos electrónicos o sitios web falsificados, lo que puede llevar a la divulgación de información valiosa (Mouradian & Choo, 2020).

Fugas de información. Las fugas de información ocurren cuando datos confidenciales se exponen o divulgan sin autorización. Estas fugas pueden ser el resultado de errores en la configuración de seguridad, violaciones de la política de seguridad de la empresa o acciones maliciosas de empleados o atacantes externos (Kalloniatis, Kavakli, & Gritzalis, 2017).

Ataques de denegación de servicio (DoS). Los ataques de denegación de servicio tienen como objetivo abrumar los recursos de una red o sistema, impidiendo que los usuarios legítimos accedan a ellos. Estos ataques pueden ser realizados por atacantes externos o mediante el uso de botnets, y pueden causar interrupciones en las operaciones comerciales (Bhatia, Pahuja, & Singhal, 2018).

Violaciones de seguridad de la nube. Con el aumento del uso de servicios en la nube, las empresas enfrentan riesgos asociados con la seguridad de los datos almacenados en la nube. Estos riesgos pueden incluir accesos no autorizados, fugas de datos, falta de cumplimiento normativo y dependencia de terceros para la seguridad de la infraestructura (Rahaman, Shrestha, & Nanda, 2020).

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1. TIPO DE INVESTIGACIÓN

Para Cívicos y Hernández (2007), la investigación descriptiva se caracteriza porque implica observar y describir el comportamiento de un sujeto sin intervenir sobre él de ninguna manera, por lo que, de acuerdo a lo mencionado, este trabajo de investigación es de **tipo descriptivo**.

3.2. NIVEL DE INVESTIGACIÓN

Hernández Sampieri et al. (2014) señalan que los estudios descriptivos persiguen la especificación de las propiedades, características y perfiles significativos de personas, grupos, comunidades o cualquier otro fenómeno analizado. Una función primordial de la investigación descriptiva es seleccionar las características esenciales del objeto de estudio y proporcionar una descripción detallada de sus partes, categorías o clases. En muchos casos, la investigación descriptiva es la elección común para aquellos que se inician en la actividad investigativa, siendo frecuente encontrarla en trabajos de grado, pregrados y diversas maestrías. Estos estudios exhiben, relatan, reseñan o identifican hechos, situaciones y rasgos característicos del objeto de estudio, y también pueden implicar el diseño de productos, modelos, prototipos, guías, entre otros.

Según Carrasco (2019), la investigación descriptiva se apoya principalmente en técnicas como encuestas, entrevistas, observación y revisión documental. Este enfoque de investigación se centra en el estudio, análisis, descripción y especificación de situaciones y características de personas, grupos, comunidades u otros fenómenos u objetos sujetos a análisis. Basándonos en esta consideración, se puede identificar el nivel de **investigación como descriptivo.**

3.3. DISEÑO DE LA INVESTIGACIÓN

De acuerdo con Hernández Sampieri et al. (2014), la investigación no experimental implica la ausencia de manipulación intencionada de las variables. En cambio, se centra en la observación de los fenómenos tal como ocurren en su contexto natural, seguida de un análisis posterior (p. 191).

Carrasco (2019) señala que el diseño de investigación transversal descriptivo se emplea para analizar y conocer las características, cualidades internas y externas, propiedades y rasgos esenciales de los hechos y fenómenos en un momento determinado. De manera similar, Hernández et al. (2014) definen la investigación de diseño transversal como aquella en la que se recolectan datos en un único momento o tiempo, con el propósito de describir variables y analizar los hechos en su estado actual. Los instrumentos de recolección de datos se utilizan de manera única durante el proceso de investigación. En este estudio, es necesario explorar procesos, examinar características, estudiar rasgos y comprender funcionalidades para obtener los datos necesarios para construir un modelo operativo. Por consiguiente, el diseño de investigación adoptado se caracteriza como **no experimental** y **de tipo transversal descriptivo.**

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

Todos los Sistemas de Detección de Intrusos (IDS) Open Source.

3.4.2. Muestra

Monitor de seguridad de red Zeek Open Source.

3.5. VARIABLES Y DIMENSIONES

3.5.1. Definición conceptual de las variables

3.5.1.1. Monitor de Seguridad de Red Zeek Open Source

Herramienta de análisis de tráfico de red de código abierto que opera de manera pasiva.

- ***Controladores de eventos de red.*** Son componentes fundamentales del monitor de seguridad de red Zeek Open Source diseñados para capturar y analizar los eventos de red en tiempo real. Estos eventos pueden incluir datos como direcciones IP, puertos de origen y destino, protocolos utilizados, flujos de comunicación y contenido de los paquetes.

  La flexibilidad de los controladores de eventos de red de Zeek permite adaptar y personalizar la detección y el análisis de eventos según las necesidades específicas de cada entorno empresarial.
- ***Intérprete de políticas de script.*** Permite definir reglas y condiciones personalizadas para el análisis y la reacción a los eventos de red capturados. Al utilizar el lenguaje de

script de Zeek, los administradores de seguridad pueden adaptar Zeek a sus necesidades específicas y fortalecer la seguridad de la red empresarial mediante la implementación de políticas de seguridad personalizadas.

- ***Motor de eventos.*** Es el núcleo del monitor de seguridad de red. Se encarga de procesar, analizar y evaluar los eventos generados por los controladores de eventos y las políticas de script de Zeek. Puede realizar comparaciones, filtros y acciones específicas en función de las reglas y directivas establecidas. Esto permite la detección de actividades maliciosas, la generación de alarmas y la toma de medidas proactivas para garantizar la seguridad de la red empresarial.

3.5.1.2. Seguridad empresarial

Se refiere a las medidas y estrategias implementadas por una organización para proteger sus activos, tanto físicos como digitales, de posibles amenazas internas y externas.

- ***Ciberseguridad.*** En el contexto de la seguridad empresarial, la ciberseguridad aborda la protección de los activos digitales y la infraestructura tecnológica utilizada por una organización. Incluye la protección de la información sensible, la prevención del acceso no autorizado, la mitigación de ataques de malware, el monitoreo de actividades sospechosas y la gestión de incidentes de seguridad.

3.5.2. Definición operacional de las variables

3.5.2.1. Primera variable descriptiva de interés

Monitor de Seguridad de Red Zeek Open Source.

Dimensiones.

- Controladores de eventos de red.
- Intérprete de políticas de script.
- Motor de eventos.

3.5.2.2. Segunda variable descriptiva de interés

Seguridad empresarial.

Dimensión.

- Ciberseguridad.

3.6. TÉCNICAS E INSTRUMENTOS PARA EL TRATAMIENTO DE DATOS

3.6.1. Técnicas e instrumentos de recolección de datos

3.6.1.1. Técnicas

- Análisis documental.
- Análisis de registros de eventos

3.6.1.2. Instrumentos

- Fichas.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

5.1. ANTECEDENTES DE LA EMPRESA

La empresa NNOVATECH E.I.R.L. fue fundada por Grover Quispe Yaulli, quien en la actualidad es el gerente general y representante a nivel funcional, en la ciudad de Ayacucho el 08 julio de 2017 con nombre comercial NT TECNOLOGIES, año en el que también inició sus actividades comerciales brindando servicio de venta de equipos de uso doméstico y reparación de los mismos.

5.1.1. Estructura organizacional

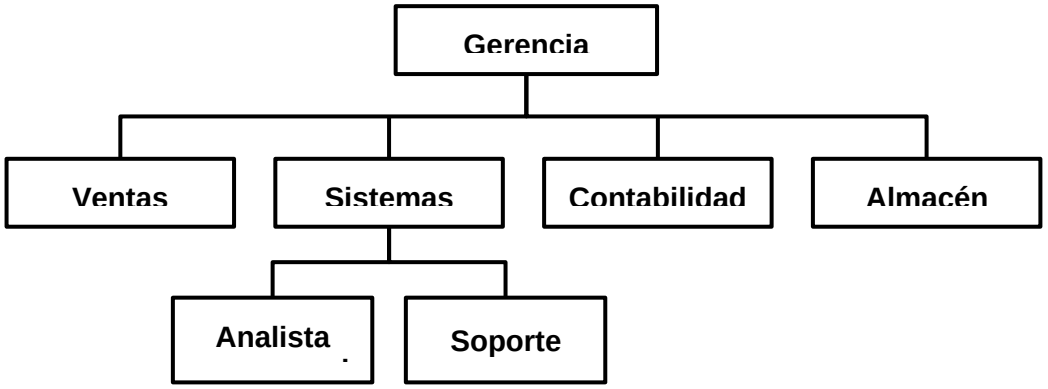
La empresa NNOVATECH E.I.R.L, está conformada por las siguientes áreas principales:

- ***Gerencia General.*** Este cargo es representativo ya que los socios son los que deciden en la empresa previa coordinación. La persona que ocupa el cargo de gerente general es responsable de velar por el correcto funcionamiento de la compañía y lograr los objetivos propuestos.
- ***Ventas.*** Esta área está encargada de las funciones comerciales, se dedica al rubro de compra y venta de equipos. Las principales actividades que se realizan en esta área es la búsqueda y aprobación o rechazo de proveedores, además de las ventas a los clientes.
- ***Almacén.*** En esta área se almacenan los equipos que se compraron, manteniendo el inventario, para su posterior venta al por mayor o menor a los diferentes clientes.

A continuación, en la Figura 2, se muestra el organigrama de esta empresa.

Figura 2

Organigrama de la empresa NNOVATECH E.I.R.L.



5.1.2. Situación actual de la infraestructura de red

La empresa NNOVATECH E.I.R.L cuenta con los siguientes dispositivos:

Tabla 3

Dispositivos pertenecientes a la empresa y sus respectivas características.

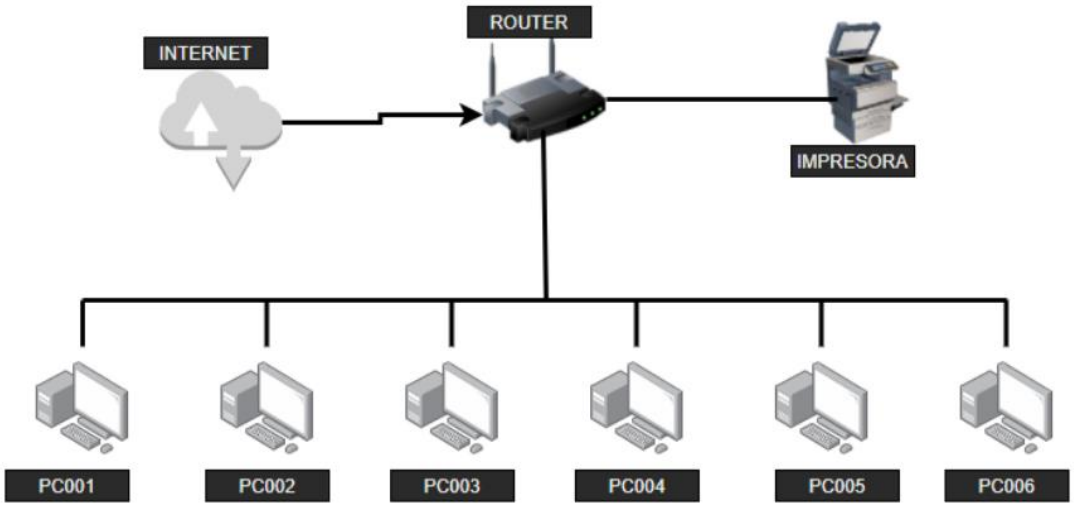
Dispositivo	Características
PC-01(Gerencia)	Marca: Lenovo Modelo: Lenovo IdeaPad 3(17) Procesador: Intel Core i5 Disco duro: 1TB RAM: 8GB Sistema Operativo: Windows 10 Home
PC-02(Ventas)	Marca: Asus Modelo: Asus 14 E410MA Procesador: Intel Core i5 Disco duro: 1 TB RAM: 4 GB Sistema Operativo: Windows 10 Home
PC-03(Programador)	Marca: Lenovo Modelo: IdeaPad 320-14ISK Procesador: Intel Core i5 Disco duro: 1TB RAM: 8GB Sistema Operativo: Windows 10 Home
PC-04(Soporte)	Marca: Lenovo Modelo: Lenovo IdeaPad 3(14) Procesador: Intel Core i5

	Disco duro: 1TB RAM: 8GB Sistema Operativo: Windows 10 Home
PC-05(Almacén)	Marca: Lenovo Modelo: Lenovo IdeaPad Flex 5 Procesador: Intel Core i5 Disco duro: 128 Solid GB RAM: 8GB Sistema Operativo: Windows 10 Home
PC-06(Contabilidad)	Marca: Asus Modelo: Asus 14 E410MA Procesador: Intel Core i5 Disco duro: 128 Solid GB RAM: 8 GB Sistema Operativo: Windows 10 Home
Router Cisco SG110D-08-8-Port	Funciones de alto rendimiento con un rendimiento gigabit potente a un precio asequible, a la vez que impulsan la velocidad y la capacidad de la red. Una amplia gama de modelos Proporciona alimentación a teléfonos IP, puntos de acceso y otros dispositivos.
Impresora Canon PIXMA G2160	Impresora multifuncional serie G, con ventajas de las impresoras multifuncionales de tinta continua para poder imprimir.

La estructura de red de la empresa se visualiza en la Figura 3, el internet llega a través del router, al cual están conectados 6 ordenadores a través de cableado UTP, al igual que la impresora.

Figura 3

Estructura de la red de la empresa.



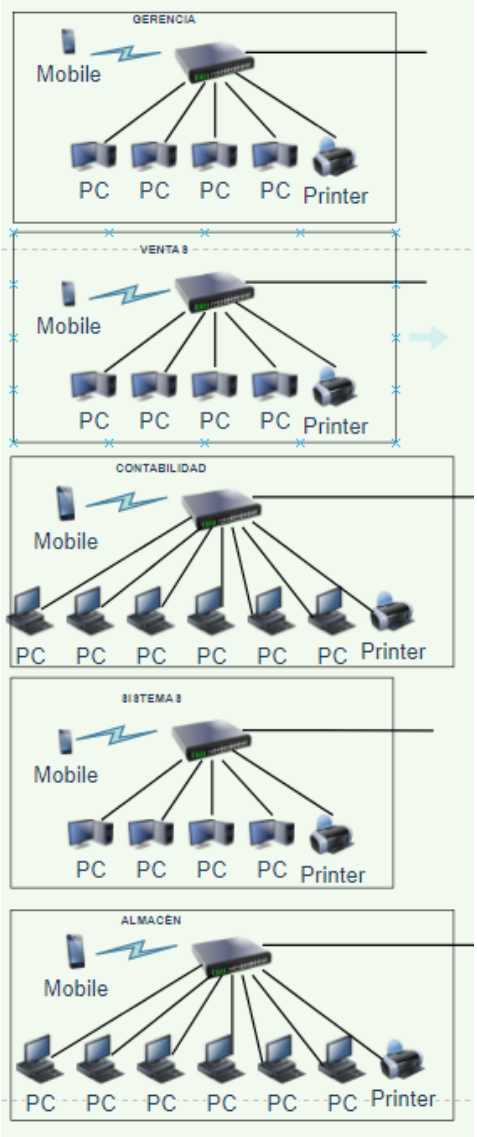
5.2. DISEÑO DE IMPLEMENTACIÓN

La estructura de red está diseñada de acuerdo al organigrama de la empresa:
gerencia, ventas, sistemas, contabilidad y almacén. las áreas mencionadas conforman capas de acceso como se muestra en la Figura 4.

Se utiliza la topología estrella, donde las conexiones entre diferentes equipos finales y el switch es de punto a punto, los access point puede tener conexión con los dispositivos por medios de guiados, y para cada área varía la cantidad de ordenadores, los que se conectan mediante switch y cableado UTP con conectores RJ45, mientras para los dispositivos como móvil o tabletas la conexión es a través de Wifi y el access point.

Figura 4

Estructura de red a nivel de capa de acceso.



A continuación, se listan los dispositivos de entrada y salida que se tienen en cuenta en la anterior estructura propuesta, además del medio.

Tabla 4

Dispositivos de entrada y salida de red a nivel de capa de acceso.

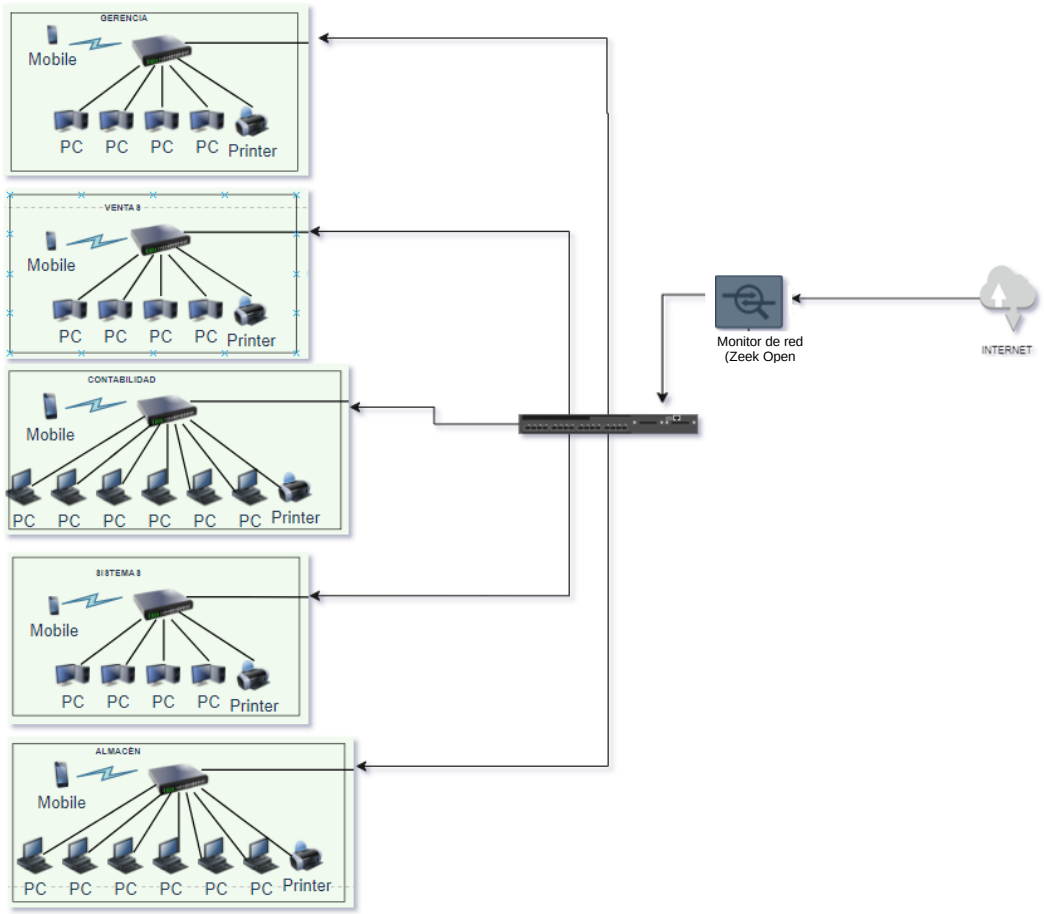
Dispositivo de entrada	Medio	Dispositivo de salida
PC01	Cable UTP (guiado)	Switch
PC02	Cable UTP (guiado)	Switch
PC03	Cable UTP (guiado)	Switch

PC04	Cable UTP (guiado)	Switch
PC05	Cable UTP (guiado)	Switch
PC06	Cable UTP (guiado)	Switch
Impresora	Cable UTP (guiado)	Switch
Móvil	Wifi (no guiado)	Access Point

La ubicación del dispositivo con el monitor de red, Zeek Open Source, es un punto estratégico, para detectar todas las amenazas externas que pretenden acceder a la red local de la empresa, como se puede ver en la Figura 5.

Figura 5

Estructura de red con la implementación del monitor.



5.3. CONFIGURACIÓN DEL ENTORNO DE PRUEBA

El entorno de prueba se realizará en un entorno virtual de VirtualBox que simulará la real, contando con:

- Una máquina host cuyo sistema operativo es Windows
- Una máquina virtual que cuenta con sistema operativo Lubuntu en la cual se instalará y desplegará Zeek.
- Una máquina virtual con sistema operativo Kali Linux para realizar los ataques o infiltraciones a la red.

La instalación de máquinas virtuales las podemos encontrar en los anexos A y B.

5.3.1. Configuración de la red

En vista que en el presente trabajo se utiliza VirtualBox para el despliegue de la(s) máquina(s) que se conectarán al dispositivo con Zeek, se configura la red de la siguiente forma:

Figura 6

Creación de la red

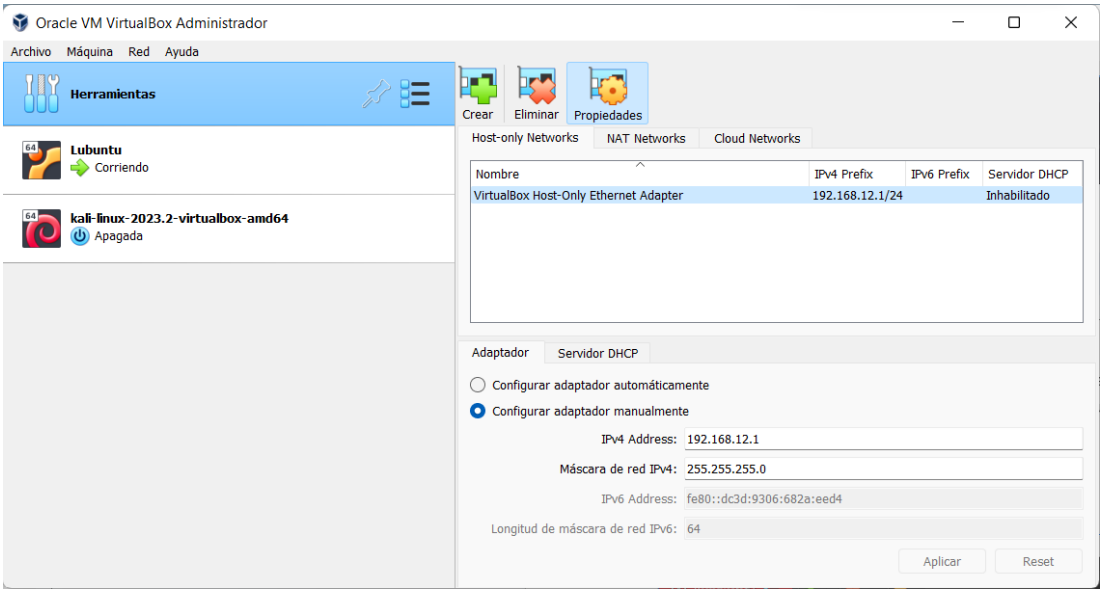


Figura 7

Configuración del primer adaptador de la máquina que tendrá instalado Zeek.

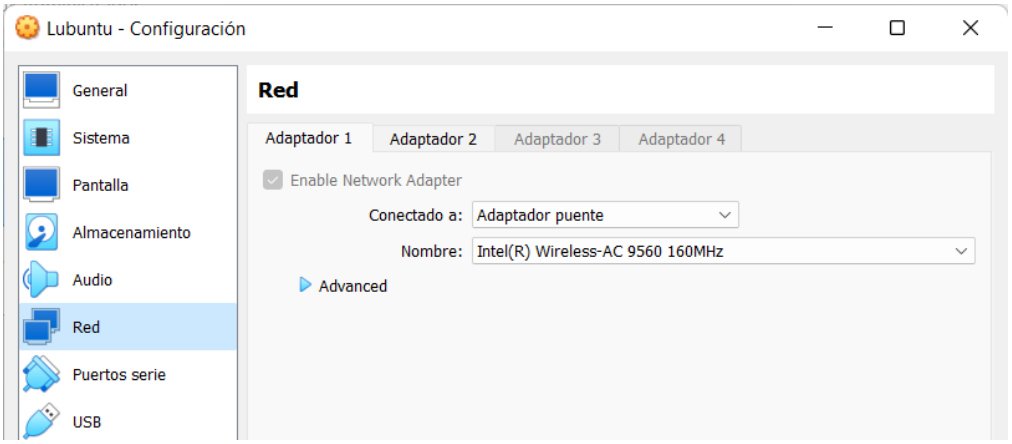
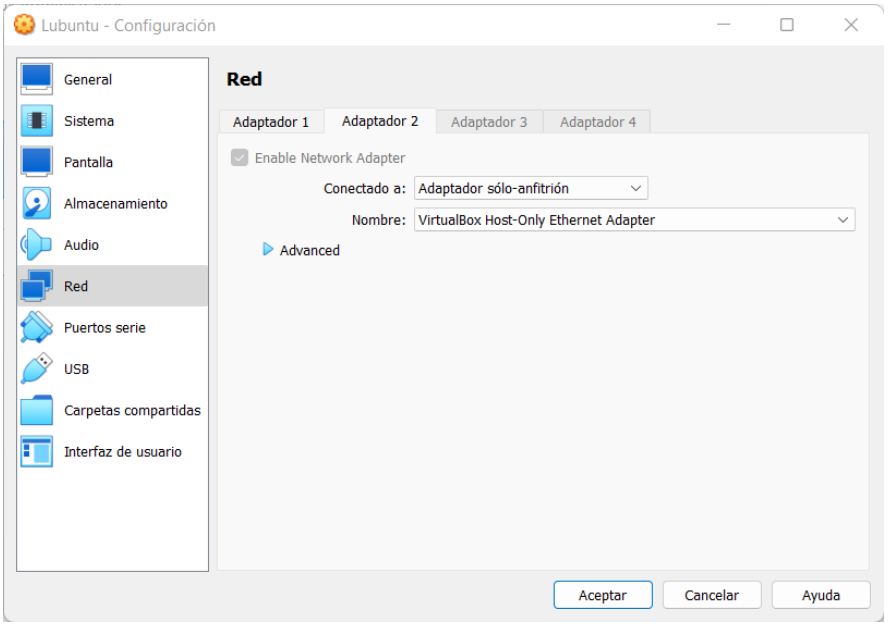


Figura 8

Configuración del segundo adaptador de Win10.



5.4. INSTALACIÓN Y CONFIGURACIÓN DE ZEEK OPEN SOURCE

5.4.1. Instalación de Zeek

La versión de Zeek a instalarse es la LTS para Ubuntu 22.04, cuyos comandos y/o pasos de instalación se muestran a continuación:

Tabla 5

Comandos a ejecutar en la terminal de la máquina en la que se instalará Zeek Open Source

Paso N°	Descripción o comando
1	echo 'deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04/ /' | sudo tee /etc/apt/sources.list.d/security:zeek.list
2	curl -fsSL https://download.opensuse.org/repositories/security:zeek/xUbuntu_22.04/Release.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/security_zeek.gpg > /dev/nul
3	sudo apt update
4	sudo apt install zeek-lts

Después de ejecutar estos comandos debe aparecer una interfaz como la que se muestra en la Figura 10.

Figura 9

Interfaz de información con respecto al tipo de servidor de correo requerido por el usuario o administrador de Zeek

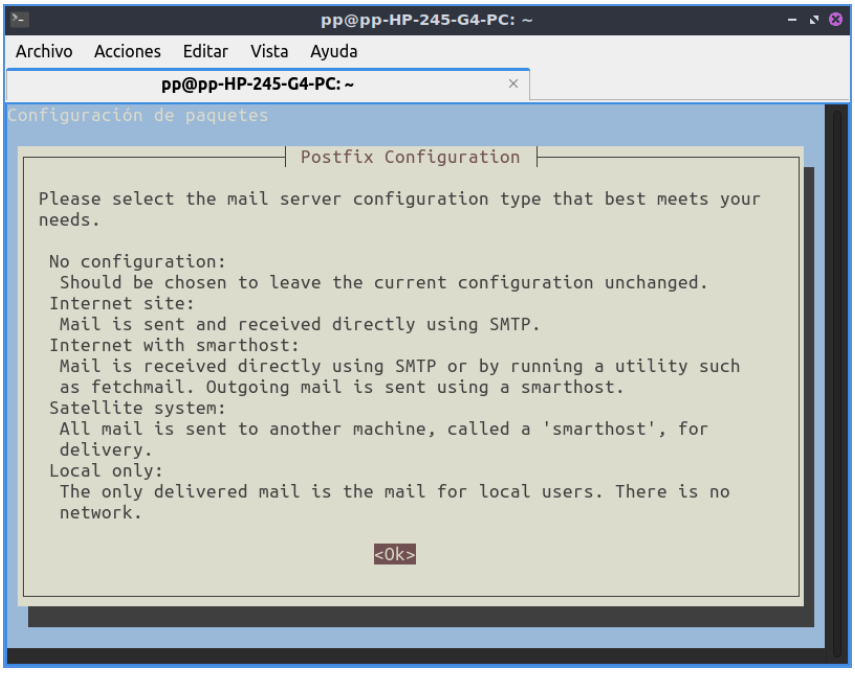


Figura 10

Interface para seleccionar la configuración de correo general

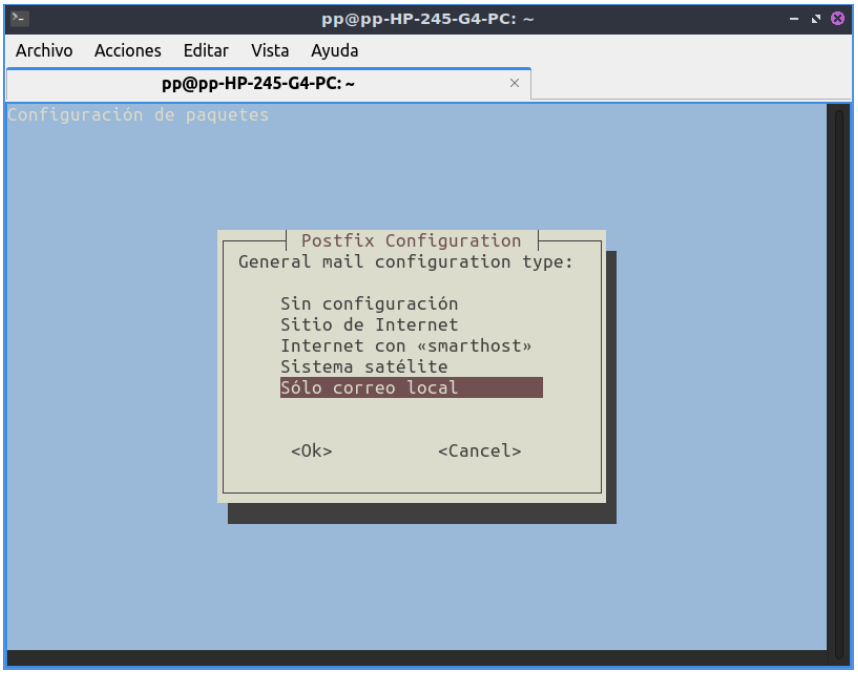
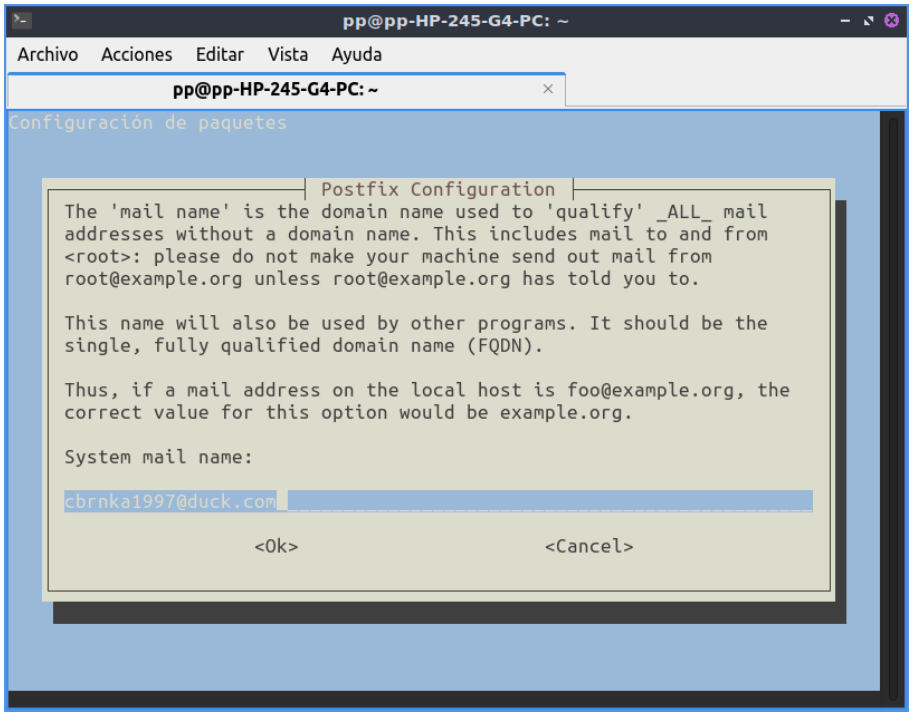


Figura 11

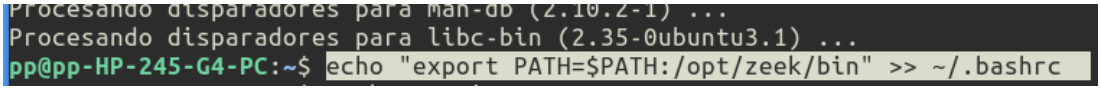
Interface que se muestra en el terminal para escoger el nombre de dominio de correo



A continuación, se debe añadir la ruta de instalación de Zeek a la variable del sistema, como se observa en la siguiente figura.

Figura 12

Se añade la ruta en la que Zeek fue instalado a la variable del sistema.



Seguidamente se procede a activar la variable de sistema con el comando source -/.bashrc y se verifica que se haya instalado Zeek como se muestra en la Figura 14.

Figura 13

Verificación de la versión de Zeek Open Source instalada.

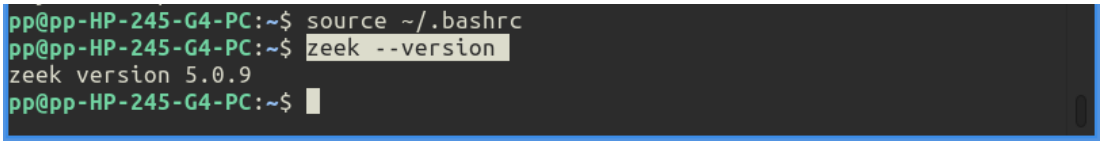
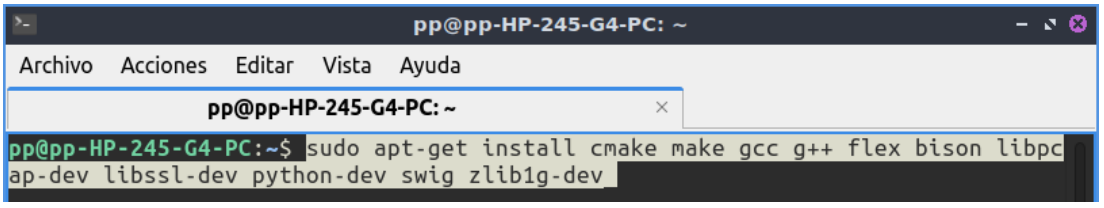


Figura 14

Instalación de las dependencias necesarias.



5.4.2. Instalación de ZeekControl

Zeek cuenta con una shell interactiva denominada ZeekControl. Para su instalación debe dirigirse al directorio en el que se instaló Zeek y ejecutar el comando de la Figura 16 como usuario root.

Figura 15

Instalación de ZeekControl.

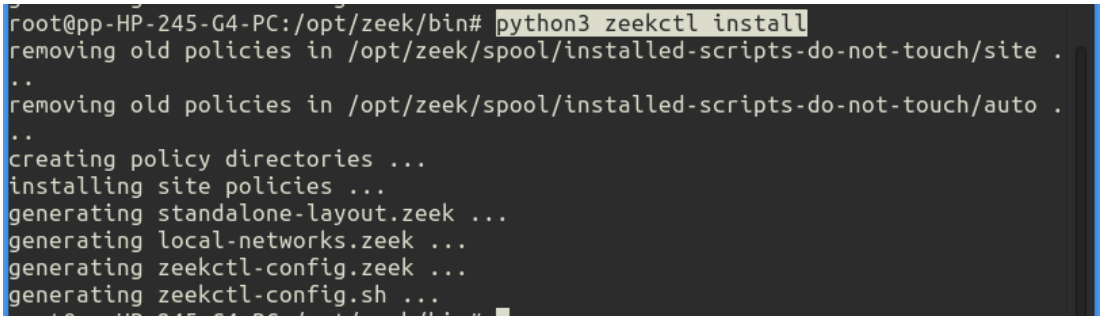


Figura 16

Validación de la instalación de ZeekControl.

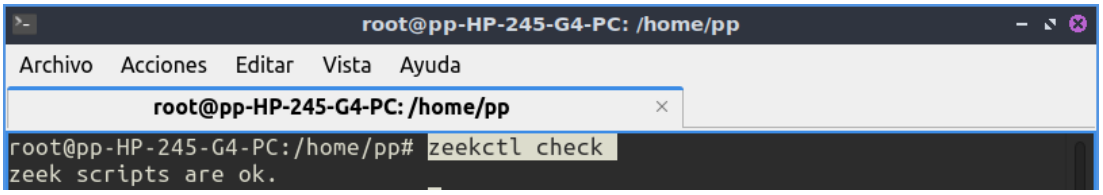
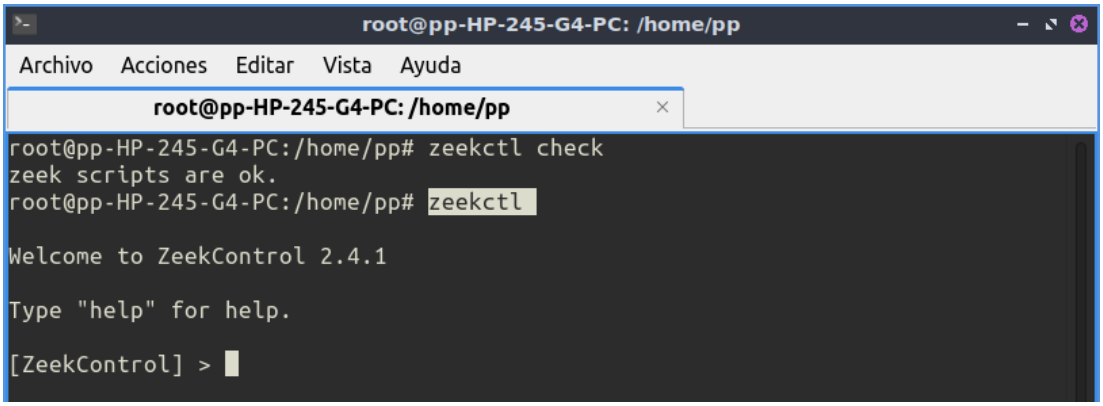


Figura 17

Ejecución de ZeekControl



5.4.3. Configuraciones mínimas de Zeek

Primero necesitamos saber la red a la que nuestra máquina virtual Zeek está conectada, la misma que de acuerdo a la interfaz gráfica es la siguiente:

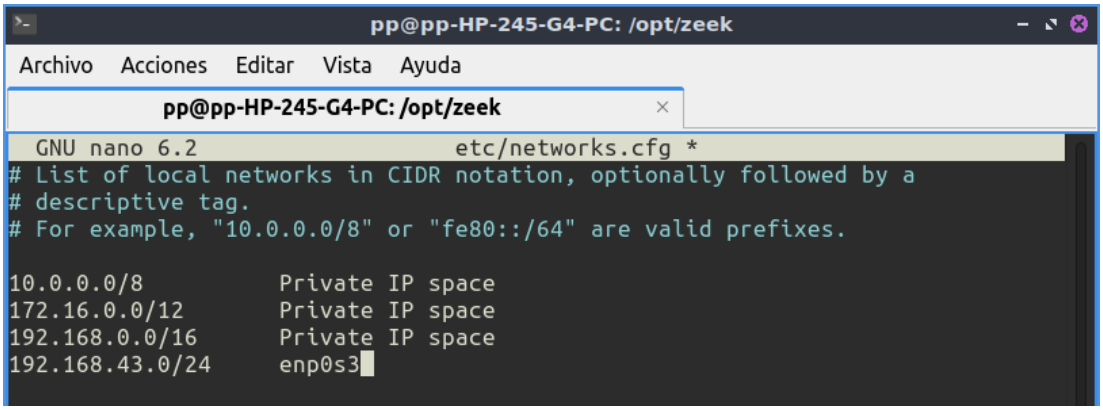
Figura 18

Red a la que la máquina virtual Zeek está conectada

Por lo que enp0s3 es la red que pondremos en los archivos de configuración de Zeek, para este fin ejecutamos el comando `sudo nano etc/networks.cfg` en consola y la añadimos como se muestra en la Figura 20.

Figura 19

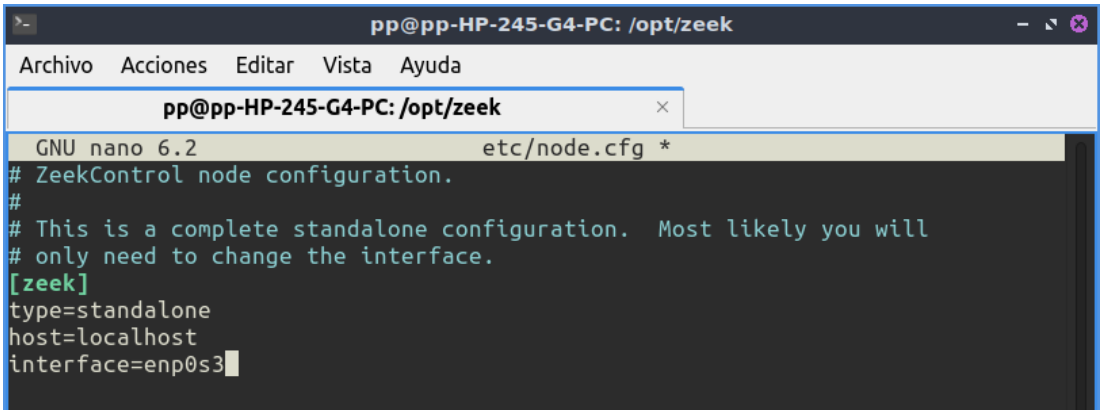
Adición de la red a ser monitorizada.



Seguidamente se ejecuta el comando `sudo nano etc/node.cfg` para añadir la red al archivo de nodo de Zeek.

Figura 20

Configuración del nodo de Zeek.

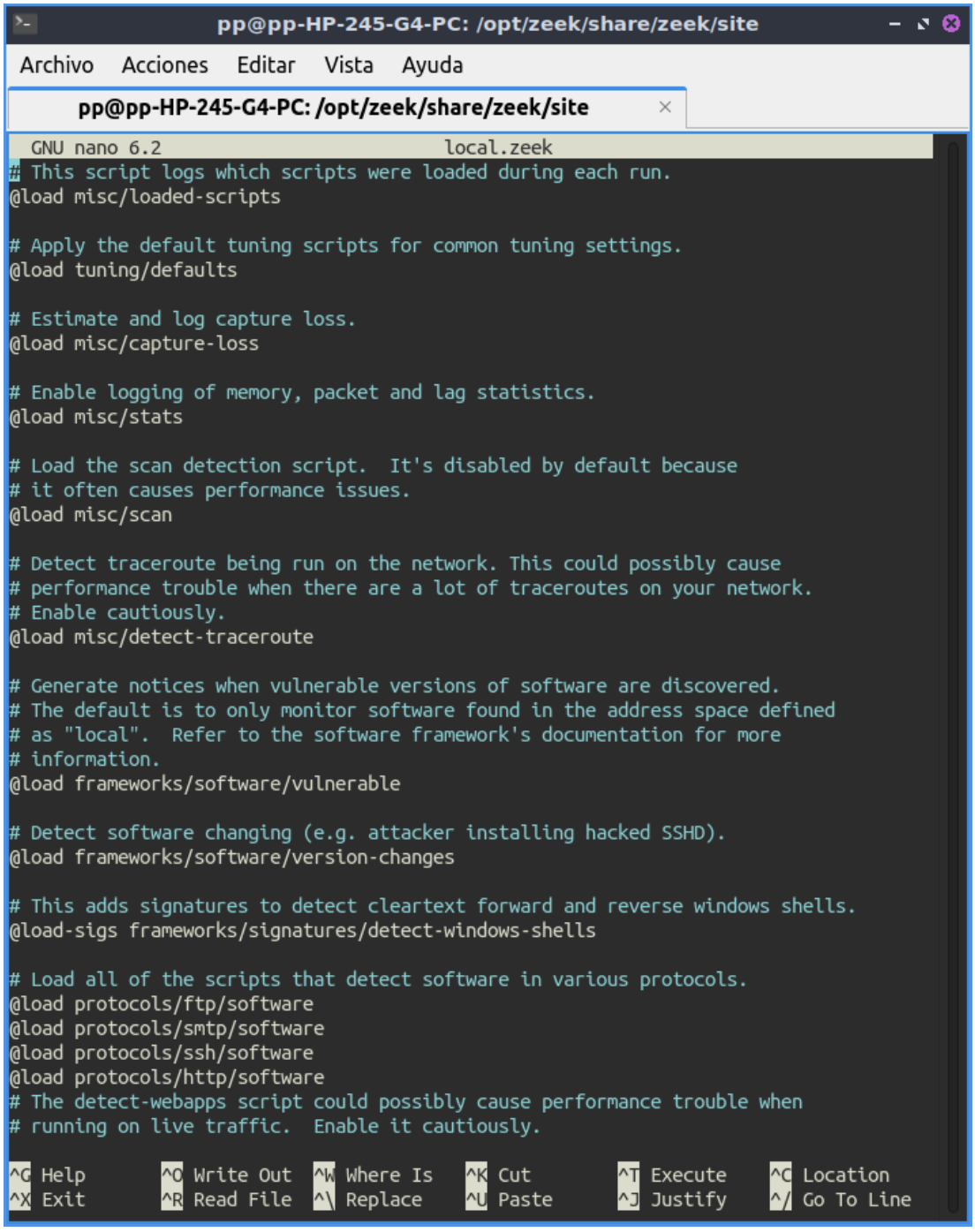


5.4.4. Políticas de Zeek

Son scripts escritos en lenguaje Zeek, que describen qué tipos de actividades se consideran sospechosas. Las políticas con las que se cuenta ahora se muestran en la Figura 22.

Figura 21

Algunas políticas de Zeek.



Todas las políticas de este archivo se encuentran en el Anexo C.

5.5. FUNCIONAMIENTO Y RECOPILACIÓN DE DATOS

5.5.1. Funcionamiento de Zeek

Figura 22

Inicialización de Zeek y comprobación de su estado.

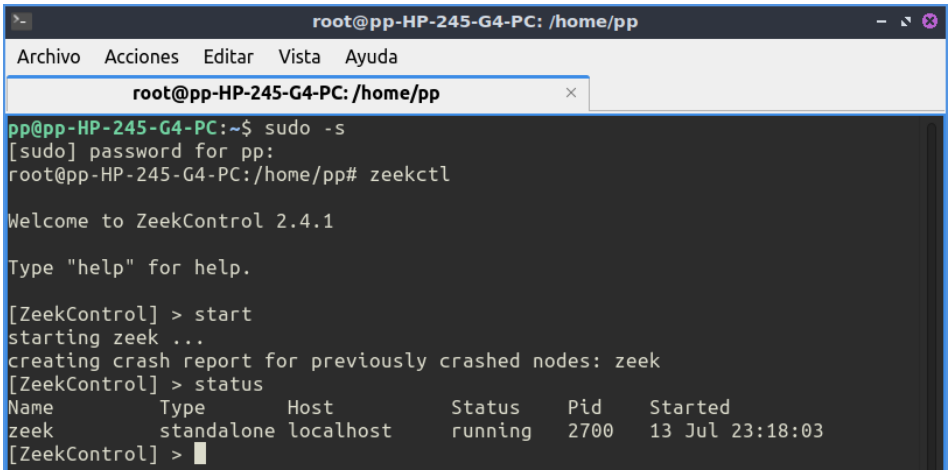
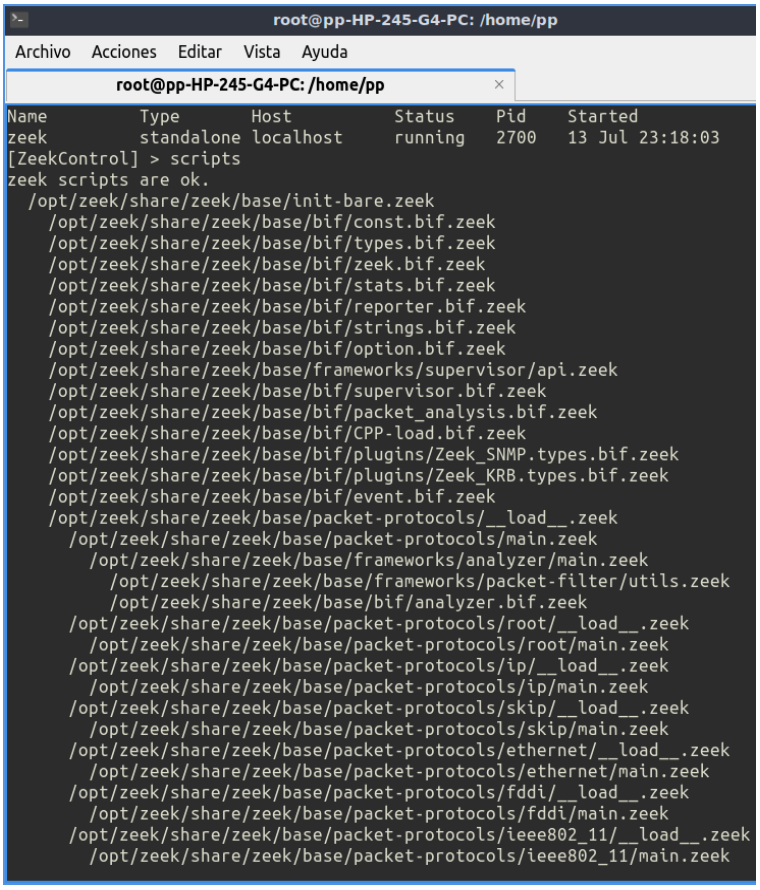


Figura 23

Comprobación de los scripts activos.



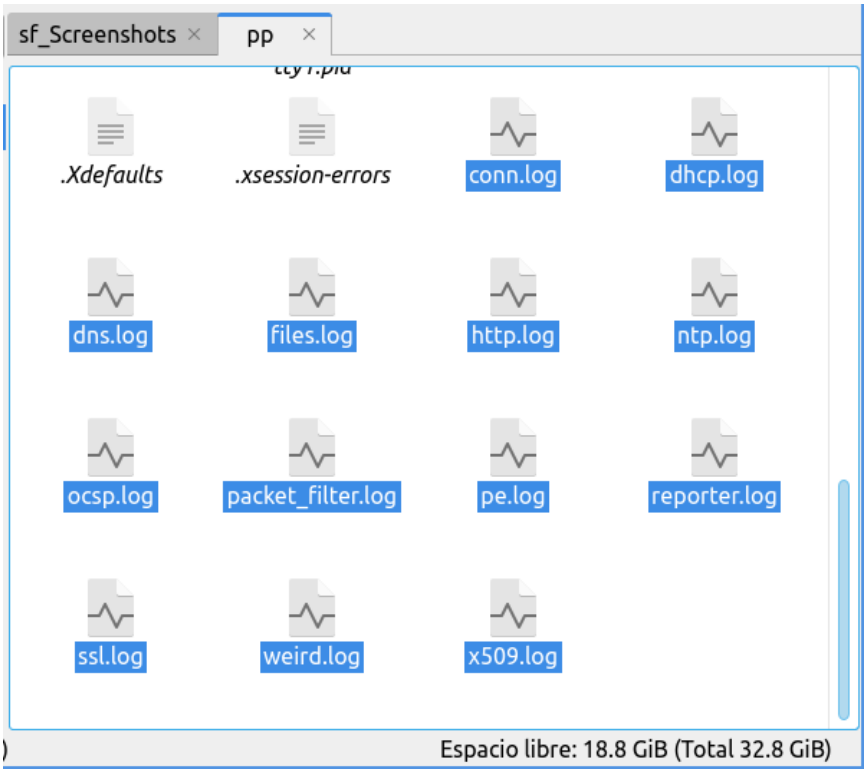
En vista que la lista de scripts es larga para mostrarse en la captura, estos son puestos en el Anexo D.

5.5.2. Recopilación de datos

Para comenzar con la recopilación de datos se ejecuta Zeek, tal como se mostró en la Figura 23. Los datos recopilados por este monitor de red se guardan en archivos .log que tienen distintas denominaciones de acuerdo a qué información contienen, tal como se puede apreciar en la Figura 25.

Figura 24

Archivos generados por Zeek.



En la Tabla 6 se describe brevemente respecto al contenido de estos archivos.

Tabla 6

Breve descripción de los archivos. logs generados por Zeek en la máquina virtual

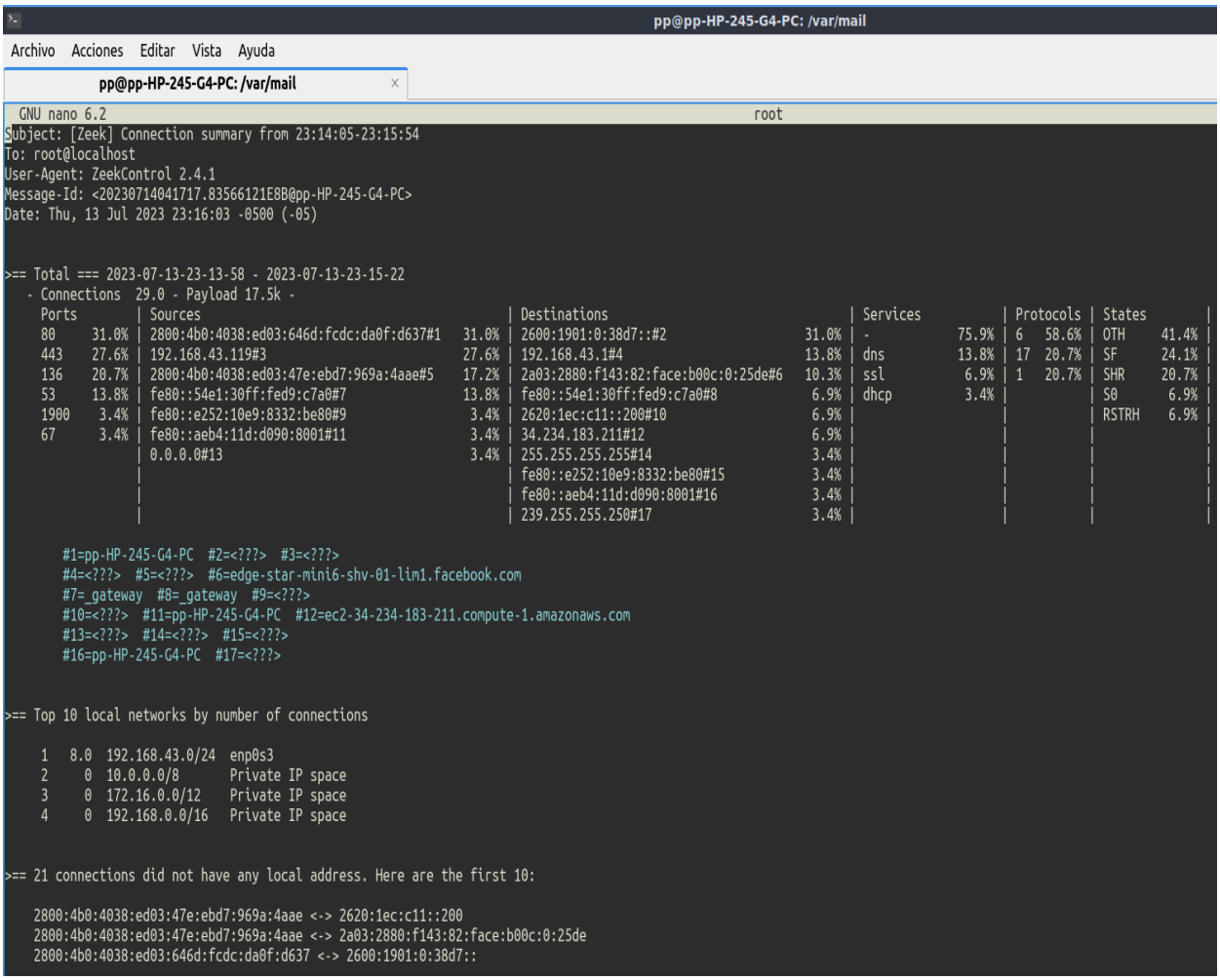
Nombre de archivo	Descripción
conn.log	Contiene una entrada para cada conexión detectada, con propiedades básicas como hora y duración, direcciones IP de origen y respuesta, servicios y puertos, entre otros. Proporciona un registro exhaustivo de la actividad de la red.
dhcp.log	Asignación de direcciones DHCP.
dns.log	Registro que ofrece información sobre cómo interactúan los sistemas con Internet y entre sí.
files.log	Registro de archivos que Zeek observó mientras inspeccionaba el tráfico de red. La existencia de una entrada en este archivo no significa que Zeek haya extraído necesariamente el

	contenido del archivo y lo haya escrito en el disco (para que esto suceda se deben realizar algunas configuraciones).
http.log	Peticiones y respuestas HTTP.
ocsp.log	Registro relacionado al Protocolo de estado de certificados en línea (Online Certificate Status Protocol - OCSP). Solo es creado cuando la política está activa, como en el presente caso.
packet_filter.log	Lista de filtros de paquetes aplicados.
pe.log	También denominado "ejecutable portátil", se encuentra asociado a los binarios de Microsoft.
reporter.log	Mensajes internos de error, advertencia y/o información.
ssl.log	Información sobre el protocolo SSL/TLS.
weird.log	Contiene actividad inusual o excepcional que puede indicar conexiones malformadas, tráfico que no se ajusta a un protocolo concreto, hardware/servicios que funcionan mal o están mal configurados, o incluso un atacante que intenta evitar/confundir un sensor.
x509.log	Captura detalles sobre los certificados intercambiados durante ciertas negociaciones TLS.

El usuario podrá obtener los primeros informes o avisos en la carpeta *mail*, dentro del archivo llamado *root*, ejemplo de este informe se ve en la Figura 26, y, en algunas ocasiones, se mostrarán mensajes en la consola.

Figura 25

Resumen de las conexiones realizadas en nuestra red el día 13 de Julio desde las 23:14:05 horas hasta las 23:15:54 horas.



En caso se desee procesar los datos con alguna herramienta, se puede cambiar el formato con el que estos se muestran, pasándolos de ASCII a JSON. Esta configuración se puede ver en el Anexo E. No obstante, también pueden ser guardados en formato TVS.

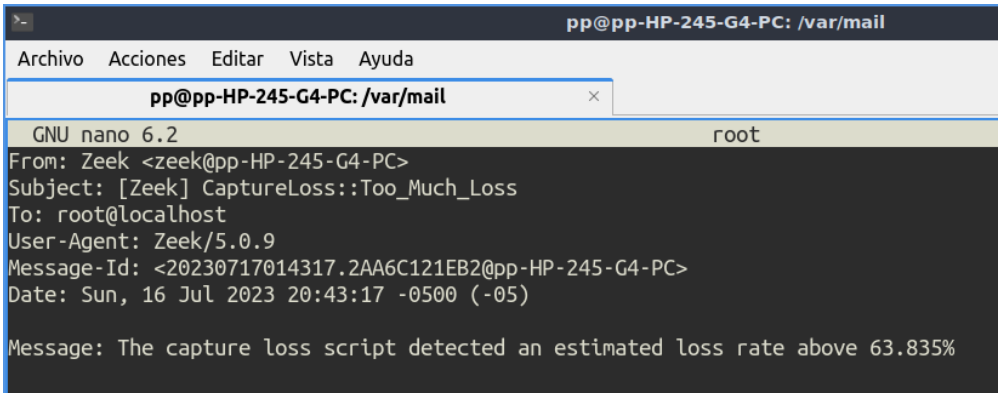
5.5.3. Notificaciones de Zeek

Además, en la mencionada carpeta y archivo se encuentran notificaciones relacionadas a otras actividades en nuestra red, tales como:

- ***CaptureLoss::Too_Much_Loss.*** Es una notificación relacionada a que la pérdida de captura detectada supera el umbral porcentual definido en la política de Zeek denominada *capture-loss.zeek.*

  Figura 26

  Pérdida detectada el día 16 de Julio a las 20:43:17 horas.

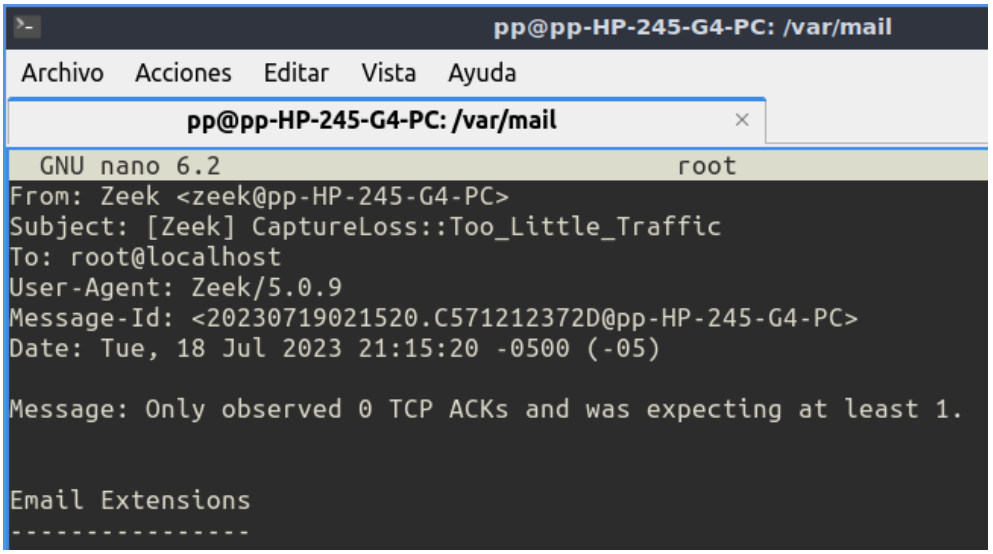


  Nota. El número de estas notificaciones llegó a 80 durante el monitoreo con Zeek durante el 13 de Julio al 01 de Agosto de 2023 (con lapsos de pausa), las cuales son adjuntadas en el Anexo F.

- ***CaptureLoss::Too_Little_Traffic.*** Reporta que el tráfico visto por un homólogo en un intervalo de vigilancia dado es menor que el número mínimo de ACKs esperados definidos en la política de Zeek denominada *capture-loss.zeek.*

  Figura 27

  Tráfico mínimo en la red el 18 de Julio a las 21:15:20 horas.

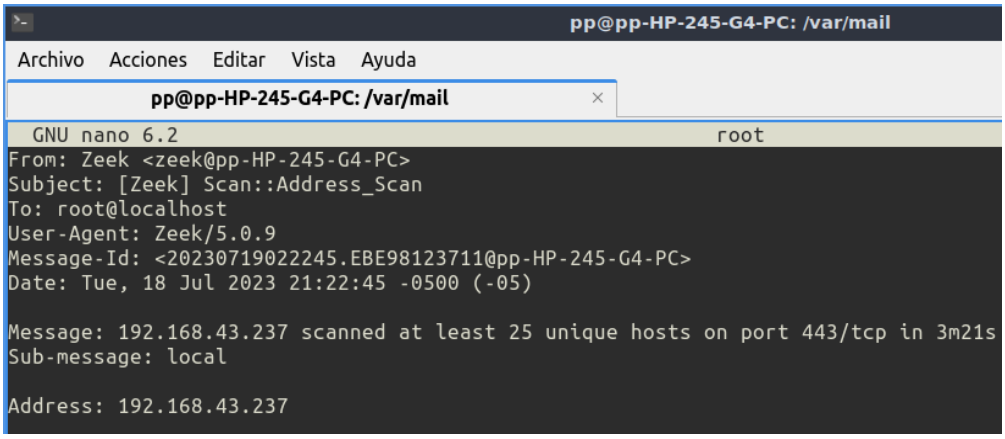


Nota. El número de estas notificaciones llegó a 7 durante el monitoreo con Zeek durante el 13 de Julio al 01 de Agosto de 2023 (con lapsos de pausa), las cuales son adjuntadas en el Anexo G.

- ***Scan::Address_Scan.*** Esta notificación da a entender que los escaneos de direcciones detectan que un host parece estar escaneando un cierto número de destinos en un único puerto. Este aviso se genera cuando un host de escaneo falla cierto número de conexiones en un único host víctima.

Figura 28

Escaneo de direcciones realizado el 18 de Julio a las 21:22:45 horas.

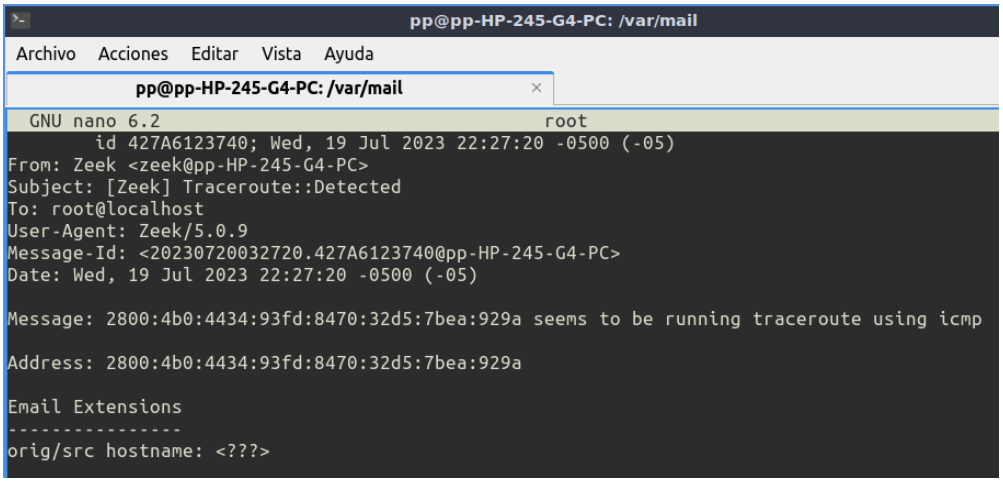


Nota. Esta notificación solo se presentó una vez durante el monitoreo con Zeek durante el 13 de Julio al 01 de Agosto de 2023 (con lapsos de pausa).

- ***Traceroute::Detected.*** Indica que un equipo en la red ha ejecutado traceroutes. Esta notificación aparece al tener activada la política *main.zeek* que se encuentra en la ruta `policy/misc/detect-traceroute/`.

Figura 29

Detección de un equipo realizando traceroutes el 19 de Julio a las 22:27:20 horas.

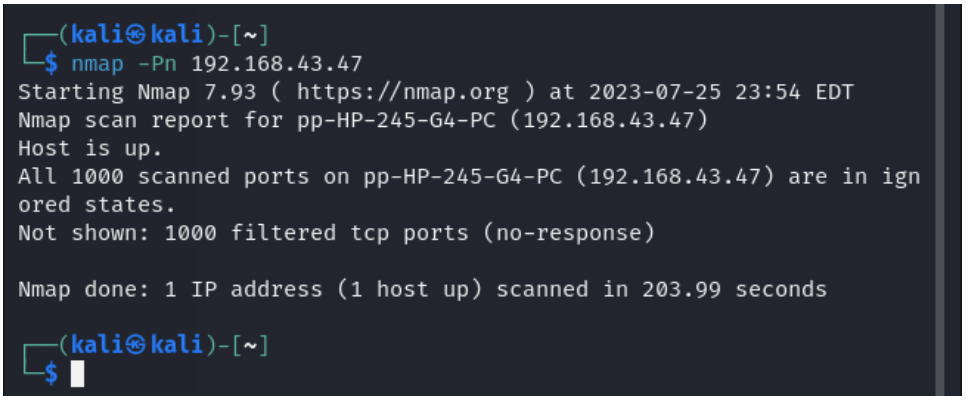


Nota. Esta notificación se presentó en dos ocasiones durante el monitoreo con Zeek durante el 13 de Julio al 01 de Agosto de 2023 (con lapsos de pausa), se encuentran adjuntadas en el Anexo H.

Para obtener otro tipo de notificación se procedió a realizar un escaneo de puertos con Kali Linux, como se ve en la Figura 31 y la respectiva notificación en la Figura 32.

Figura 30

Escaneo de puertos con Kali Linux

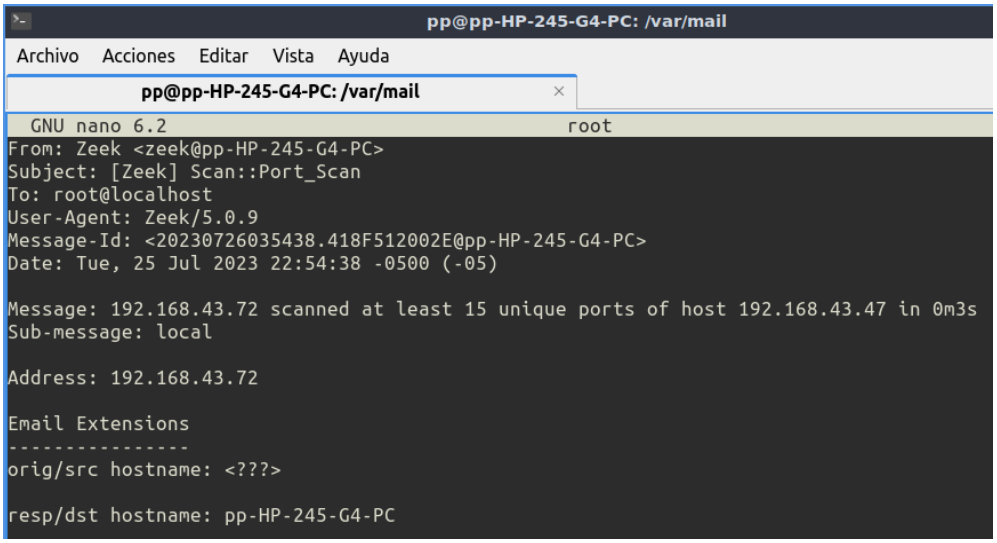


Nota. La hora en la máquina Kali Linux tiene una diferencia de 60 minutos.

- ***Scan::Port_Scan.*** Esta notificación se muestra al tener activada la política denominada scan.zeek. Detecta que un equipo atacante parece estar escaneando un único host víctima en varios puertos.

Figura 31

Atacante escaneando varios puestos del equipo o máquina víctima en nuestra red el día 25 de Julio a las 22:54:38 horas

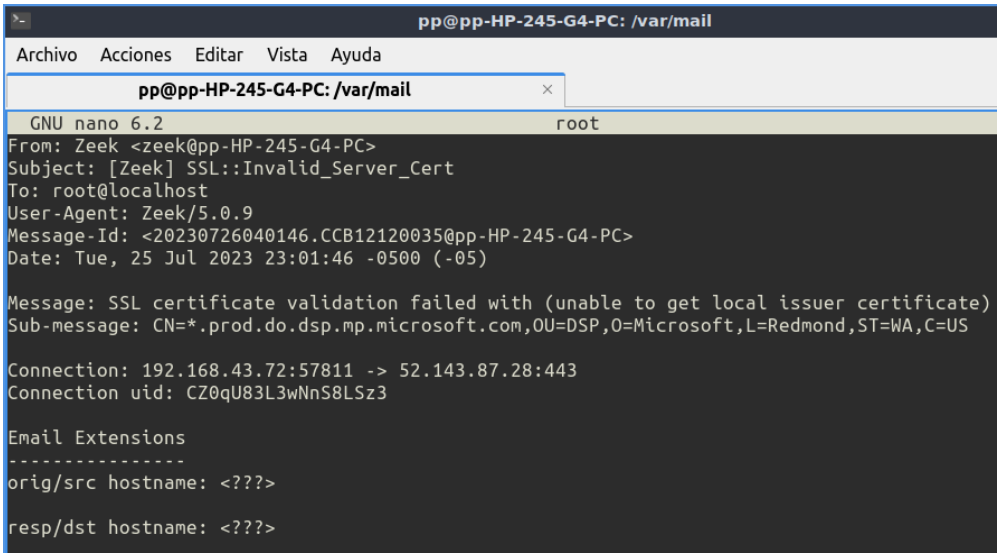


Nota. Esta notificación se presentó en cuatro ocasiones durante el monitoreo con Zeek durante el 13 de Julio al 01 de Agosto de 2023 (con lapsos de pausa), se encuentran adjuntadas en el Anexo I.

- ***SSL::Invalid_Server_Cert.*** Indica que el resultado de la validación del certificado junto con su cadena de certificado completa no era válido.

Figura 32

Validación del certificado fallido, proveniente de algún producto o servicio de Microsoft.



Nota. Esta notificación se presentó 14 veces durante el monitoreo con Zeek durante el 13 de Julio al 01 de Agosto de 2023 (con lapsos de pausa), se encuentran adjuntadas en el Anexo J.

Parte de la prueba de notificaciones fue realizar un ping con una máquina Kali Linux hacia la máquina con Zeek de la forma en la que se ve en la Figura 34 y, en la Figura 35, el mensaje de Zeek en consola respecto a los paquetes recibidos.

Figura 33

Ping realizado con Kali Linux a la máquina con IP 192.168.43.47.

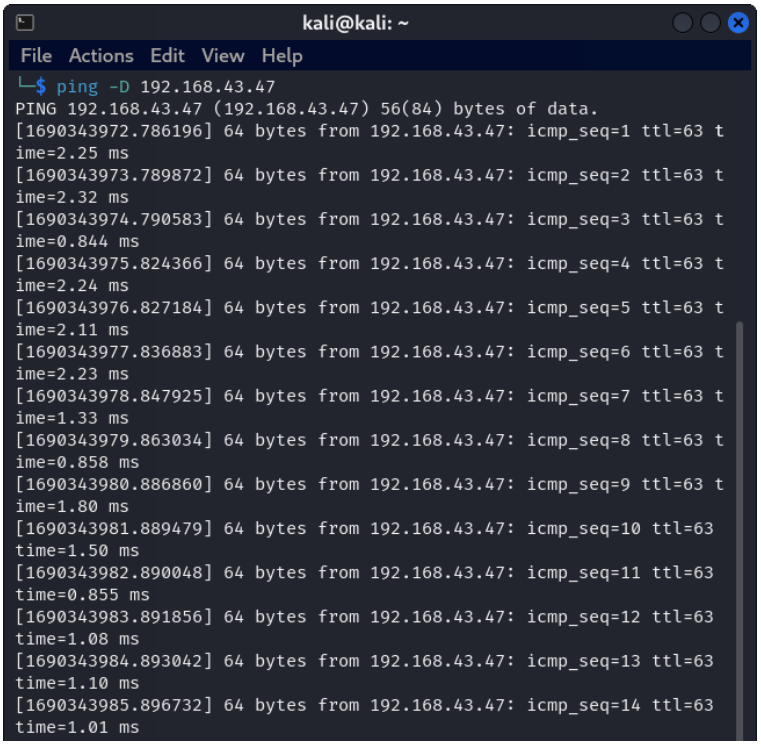


Figura 34

Paquetes recibidos producto del testing de acceso con Kali Linux.

5.6. EVALUACIÓN DEL IMPACTO EN LA SEGURIDAD EMPRESARIAL

A continuación, en la Tabla 7, y a forma de resumen se mencionan los tipos de notificaciones obtenidas por Zeek en el entorno de prueba durante el periodo comprendido entre el 13 de Julio al 01 de Agosto de 2023, cantidad, implicancia y posibles medidas de mitigación o acciones a tener en cuenta para mejorar la seguridad empresarial.

Tabla 7

Tipos de notificaciones obtenidas por Zeek, cantidad, implicancia y posibles medidas de mitigación o acciones a tener en cuenta para mejorar la seguridad empresarial

Tipo de notificación	Cantidad	Implicancia	Medida de mitigación

CaptureLoss::Too_Much_Loss	80	Puede afectar la capacidad de Zeek para analizar completamente el tráfico de red, lo que a su vez puede resultar en una detección insuficiente de actividades maliciosas o incidentes de seguridad.	Se pueden realizar ajustes en la configuración de Zeek para mejorar la captura y el procesamiento de paquetes, como aumentar el tamaño del búfer de captura, optimizar la configuración de hardware de red o reducir la carga de trabajo en el sistema.
CaptureLoss::Too_Little_Traffic	7	Podría sugerir problemas en la conectividad o problemas de rendimiento.	Investigar las causas del bajo tráfico, como problemas de red, configuraciones incorrectas o posibles ataques de denegación de servicio (DoS). Se deben realizar pruebas y/o análisis detallado del monitoreo para identificar y resolver cualquier problema que pueda estar afectando el tráfico normal de la red.
Scan::Address_Scan	1	Puede indicar un intento de reconocimiento por parte de un atacante para identificar hosts	Implementar reglas de firewall para bloquear o limitar el tráfico sospechoso de escaneo. También se puede considerar configurar sistemas de

		vulnerables.	prevención de intrusiones (IPS) para detectar y bloquear automáticamente intentos de escaneo.
Traceroute::Detected	2	Al indicar que se ha detectado un intento de trazado de ruta (traceroute) en la red, nos da a entender que este puede ser utilizado por atacantes para identificar la topología de la red y encontrar posibles puntos de vulnerabilidad.	Se puede configurar el firewall para bloquear los paquetes de trazado de ruta provenientes de direcciones IP no autorizadas. También se puede configurar el enrutador para deshabilitar la funcionalidad de trazado de ruta desde el exterior de la red.
Scan::Port_Scan	4	Puede indicar un intento de un atacante para identificar puertos abiertos y servicios vulnerables.	Configurar el firewall para bloquear o limitar el tráfico de escaneo de puertos sospechosos. Además, es fundamental mantener actualizados los servicios y aplicaciones de red para reducir la superficie de ataque.
SSL::Invalid_Server_Cert	14	Al detectar uno o varios certificados de servidor SSL inválidos en la comunicación segura,	Investigar y corregir los problemas relacionados con los certificados SSL, como la configuración incorrecta o la

	podría indicar intentos de ataque de intermediarios o certificados no confiables.	instalación de certificados de confianza. También se puede configurar Zeek para detectar y alertar sobre certificados SSL no válidos en tiempo real.

Teniendo en cuenta que las notificaciones relacionadas a la pérdida de una cantidad significativa de paquetes durante la captura de datos son muchas, se ha de tener en cuenta una mejora en la configuración de los scripts o políticas de Zeek para que se adecuen de forma óptima al entorno empresarial en el que se implementará y no dejarlo con las configuraciones por defecto. Sin embargo, y a pesar del problema de monitoreo mencionado, se logró detectar y alertar sobre diversas actividades maliciosas y problemas de seguridad, lo cual respalda la eficacia del monitoreo para proteger la red empresarial e implica un gran avance al estado inicial de nuestra red en la que se desconocía su actividad.

En general, los resultados obtenidos muestran que la implementación de Zeek fue efectiva para detectar y notificar sobre diversas amenazas y problemas de seguridad en la red empresarial. Las implicancias y medidas de mitigación asociadas con cada tipo de notificación proporcionan información valiosa para mejorar la seguridad y protección de la infraestructura de la empresa.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

A través de la implementación de Zeek Open Source y la exploración de sus componentes clave, se abordaron los problemas secundarios planteados y se lograron los objetivos específicos establecidos.

a. Se demostró que el monitor de seguridad de red Zeek Open Source basado en controladores de eventos de red es un mecanismo efectivo para la protección de las redes empresariales en entornos libres. Los controladores de eventos permiten la captura y análisis de tráfico de red en tiempo real, facilitando la detección temprana de posibles amenazas y la generación de alertas para una acción inmediata.
b. Se comprobó que el monitor de seguridad de red Zeek Open Source basado en intérpretes de políticas de script es una herramienta valiosa para la seguridad empresarial en entornos libres. Estos intérpretes de políticas permiten la personalización y adaptación del monitoreo de red según las necesidades y políticas de seguridad específicas de cada organización, fortaleciendo así la capacidad de detección y respuesta ante incidentes de seguridad.
c. Se constató que el monitor de seguridad de red Zeek Open Source basado en motores de eventos proporciona una capa adicional de protección a las redes empresariales en entornos libres. Estos motores de eventos permiten la correlación de datos y la identificación de patrones anómalos, lo que facilita la detección de amenazas sofisticadas y la generación de informes detallados para un análisis exhaustivo.

5.2. RECOMENDACIONES

a. Ha de tenerse en cuenta que Zeek es poco usable y que tiene un grado de dificultad elevado.
b. Se recomienda utilizar esta herramienta después del firewall u otro dispositivo de seguridad ya que este realiza un primer filtro. Caso contrario, se coloca después del router.
c. Se recomienda llevar a cabo la buena práctica de modificar los ajustes o configuraciones por defecto para que el monitoreo de Zeek obtenga mejores resultados.

REFERENCIAS

Ahmed, S. R., & Hassan, M. M. (2021). Network Security Monitoring: Its Benefits and Emerging Trends. *In Advances in Computer Science and Ubiquitous Computing*, 93-99.

Álvarez, A. (2015). *Análisis, Diseño e Implementación de una herramienta de Monitoreo y Control de Datacenter Basado en Herramientas OPEN SOURCE aplicado al Banco de Guayaquil* [Tesis de grado]. Universidad Politécnica Salesiana - Sede Guayaquil, Ecuador.

Álvarez, S. (2019). *Despliegue de la herramienta Zeek y su posterior explotación para el análisis de actividades sospechosas en la red* [Tesis de postgrado]. Universidad Oberta de Catalunya, España.

Barr, J. (2020). *Zeek (Bro) Network Security Monitor*. Censys Blog. https://censys.io/blog/zeek-bro-network-security-monitor

Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (1st ed.). No Starch Press.

Bejtlich, R. (2020). *The Best of TaoSecurity Blog, Volume 2: Network Security Monitoring, Technical Notes, Research, and China and the Advanced Persistent Threat*. TaoSecurity LLC.

Bernal Torres, C. A. (2010). *Metodología de la investigación: administración, economía, humanidades y ciencias sociales* (O. Fernández Palma, Ed.). Pearson Educación.

Bhatia, A., Pahuja, R., & Singhal, A. (2018). Analysis of denial of service attack and its countermeasures. *Procedia Computer Science*, (132), 891-899. 10.1016/j.procs.2018.05.133

Carrasco Díaz, S. (2015). *Metodología de la investigación científica: pautas metodológicas para diseñar y elaborar el proyecto de investigación*. San Marcos.

Chira, E. (2020, Septiembre 9). La ciberseguridad de las compañías en jaque. *El Peruano*. https://elperuano.pe/noticia/103474-la-ciberseguridad-de-las-companias-en-jaque

Cívicos, A., & Hernández, M. (2007). Algunas reflexiones y aportaciones en torno a los enfoques teóricos y prácticos de la investigación en trabajo social. *Revista Acciones e investigaciones sociales.*, (23), 25-55.

Corelight. (2021). *What is Zeek?* Corelight. Retrieved May 13, 2023, from https://corelight.com/resources/what-is-zeek

Duchene, A. (2020). *Zeek - Open Source Network Security Monitoring. The State of Security.* Tripwire. https://www.tripwire.com/state-of-security/featured/zeek-open-source-network-security-monitoring/

Fernández Collado, C., Baptista Lucio, P., & Hernández Sampieri, R. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.). McGraw-Hill Education.

ITMASTERSMAG. (2020). Retrieved May 19, 2023, from https://www.itmastersmag.com/noticias-analisis/los-%20ciberataques-que-marcaron-el-2020/

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*(2), 618-644. 10.1016/j.dss.2005.05.019

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2017). Security and privacy challenges in cloud computing environments. *Computers & Electrical Engineering*, (59), 112-129. 10.1016/j.compeleceng.2016.06.012

Kopp, J. (2020). *What is Zeek? A Powerful Network Security Monitoring Tool.* Netsurion Blog. Retrieved May 13, 2023, from https://www.netsurion.com/resources/blog/what-is-zeek

Kumar, N., & Chang, V. (2019). Research directions for malware detection and classification: A survey. *Journal of Information Security and Applications*, (44), 1-10. 10.1016/j.jisa.2018.11.011

Li, L., He, K., Chen, W., Wang, Z., Wang, Y., & Wang, X. (2019). A survey on network security monitoring and analysis techniques. *Journal of Network and Computer Applications*, (127), 9-23.

Mouradian, S., & Choo, K. K. R. (2020). A comprehensive survey on phishing attacks. *Computers & Security*, *90*(101710). 10.1016/j.cose.2019.101710

Quispe, J. (2018). *Implementación de un Sistema de Monitoreo y Control de Red, Para un Canal de Televisión, Basado en Herramientas Open Source y Software Libre* [Tesis de grado]. Universidad Nacional del Altiplano. Perú.

Rahaman, S. M. M., Shrestha, A., & Nanda, P. (2020). A review of cloud security vulnerabilities and risks in a multi-cloud environment. *Journal of Cloud Computing*, *9*(1), 1-22. 10.1186/s13677-020-00170-7

Sanders, C., & Smith, J. (2013). *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Elsevier Science.

Singh, S., & Khanuja, S. (2021). *Network Intrusion Detection using Zeek and Snort* (Confluence). 2021 11th International Conference on Cloud Computing, Data Science & Engineering.

Woody, A. (2013). *Enterprise Security: A Data-Centric Approach to Securing the Enterprise*. Packt Publishing, Limited.

Zambrano Burgos, M. A., Santisteban Avalos, E. I., Landio Rojas, R. F., & Flores Panaifo, J. M. (2019). *SISTEMA DE MONITOREO DE INFRAESTRUCTURA PARA LA 44 GESTIÓN DE RECURSOS DE TI EN LA EMPRESA COGA* [Tesis de grado]. Universidad Científica del Sur, Perú.

The Zeek Project. (n.d.). *About Zeek — Book of Zeek*. Zeek Documentation. Retrieved May 13, 2023, from https://docs.zeek.org/en/master/about.html#what-is-zeek

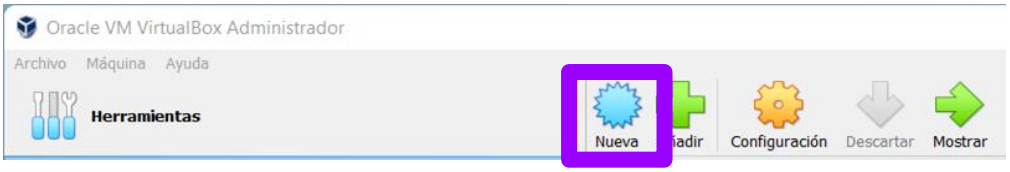
ANEXOS

ANEXO A

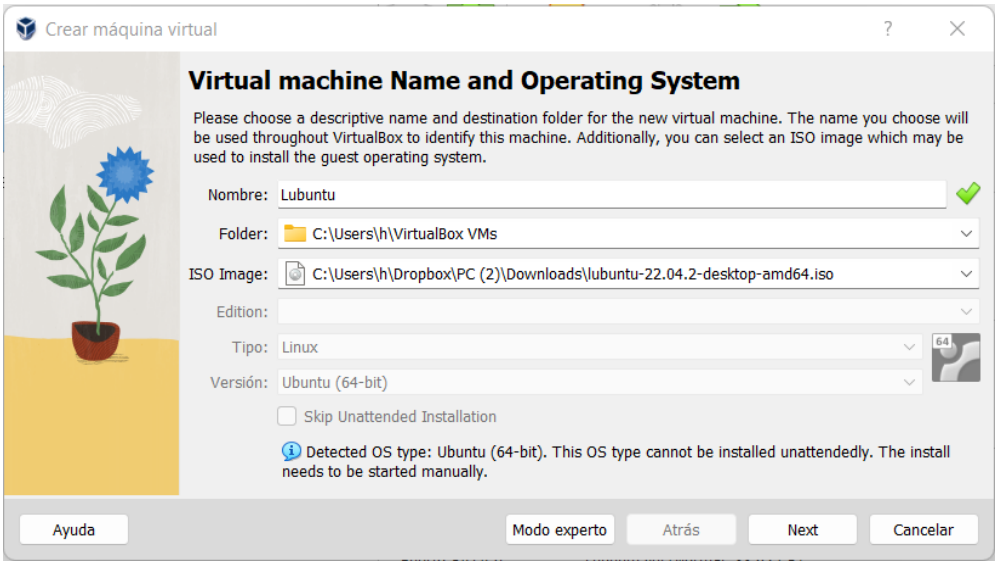
Instalación de la máquina virtual Lubuntu

1. Se descarga la imagen .iso del sistema operativo desde la página oficial: https://lubuntu.me/downloads/

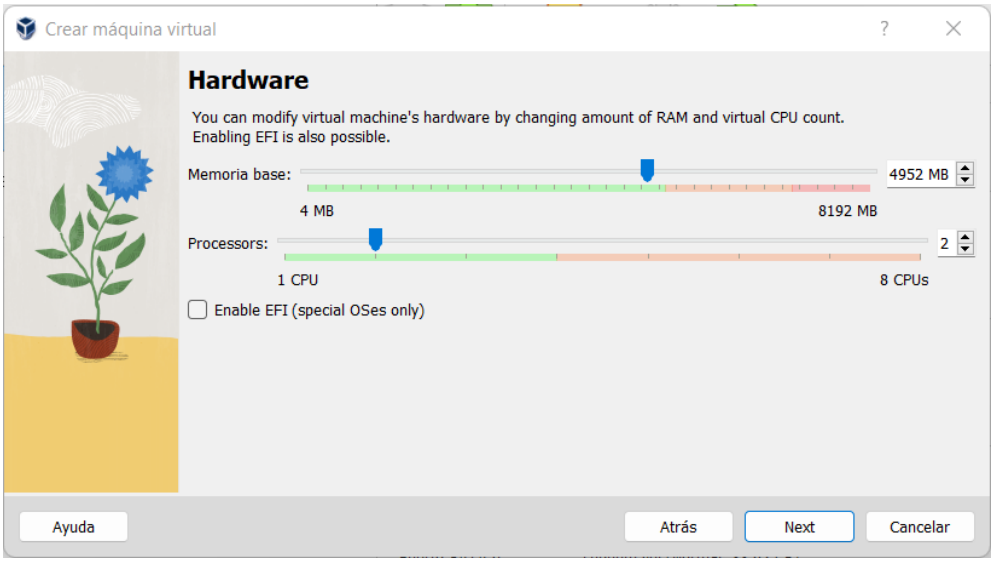
   En el presente trabajo se utilizó la versión 22.04.2 LTS (Jammy Jellyfish).
2. Estando en VirtualBox, se hace clic sobre el botón *Nueva*.



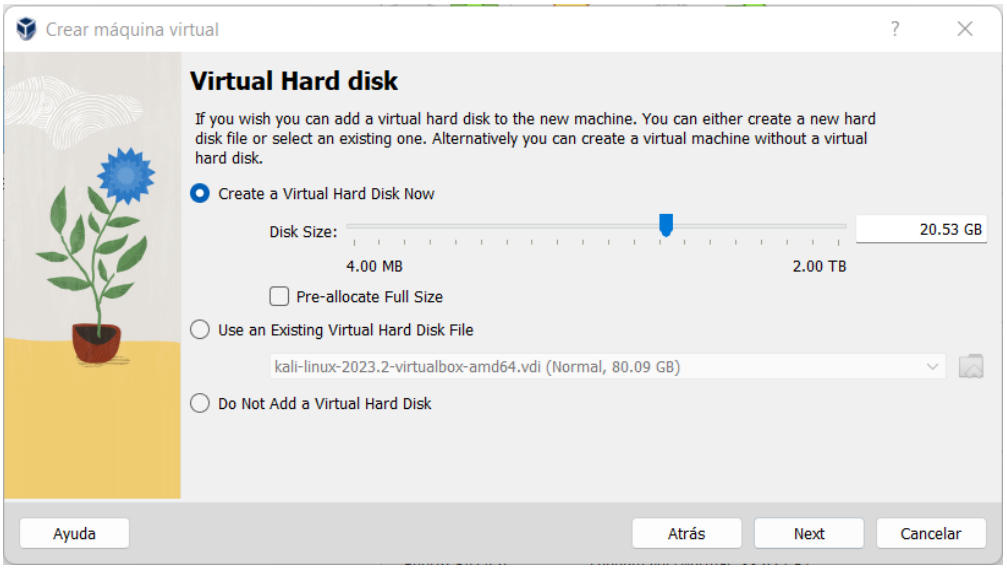
3. Aparecerá una ventana, en la que se le debe asignar un nombre a la máquina virtual y seleccionar la imagen ISO, seguidamente se da clic en el botón *Next*.



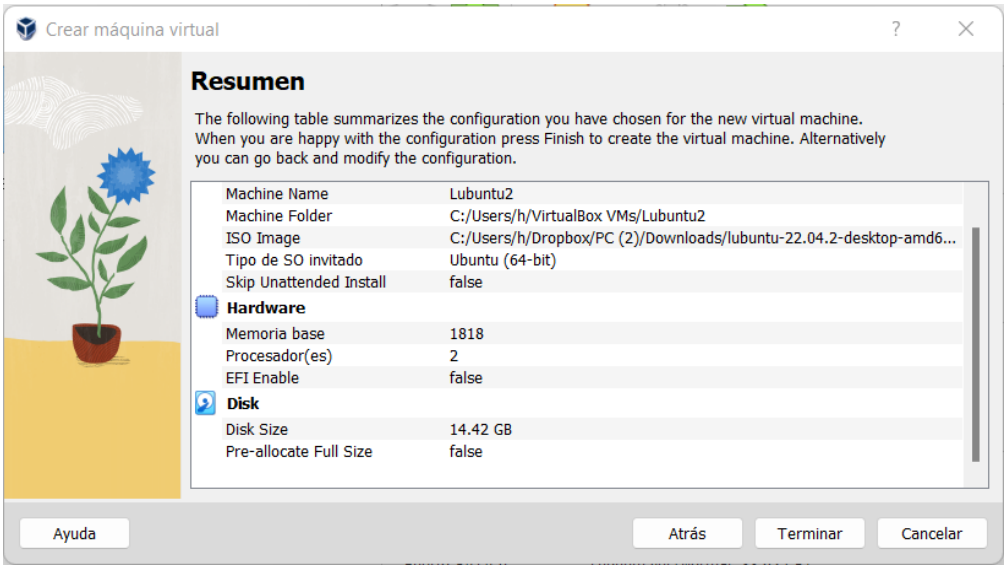
4. Se configuran las propiedades de hardware deseadas para la máquina virtual, luego se hace clic en el botón *Next*.



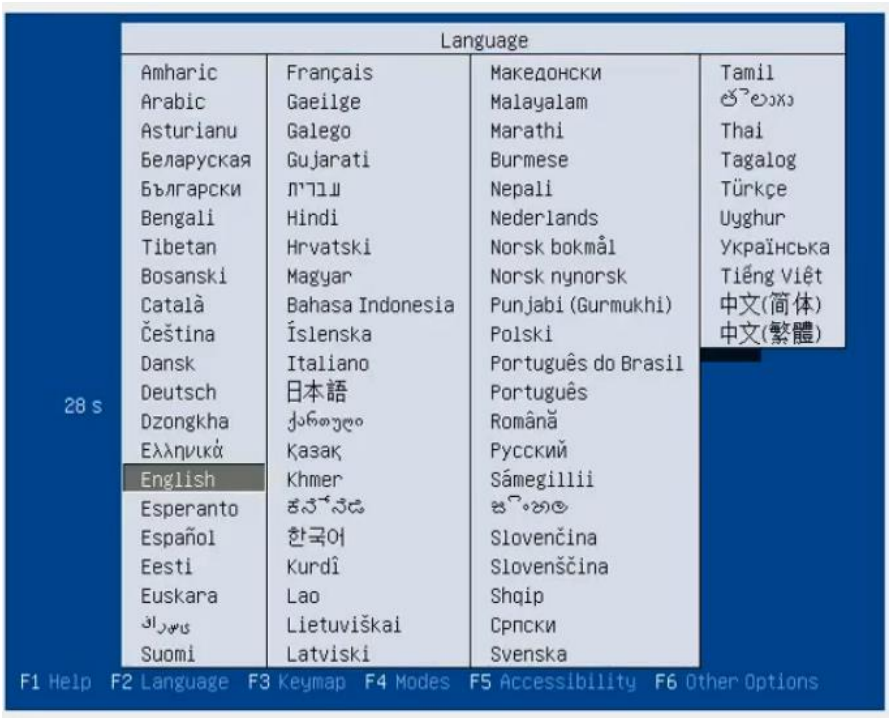
5. Se configura el tamaño de disco duro virtual, a continuación, se da clic en el botón *Next*.



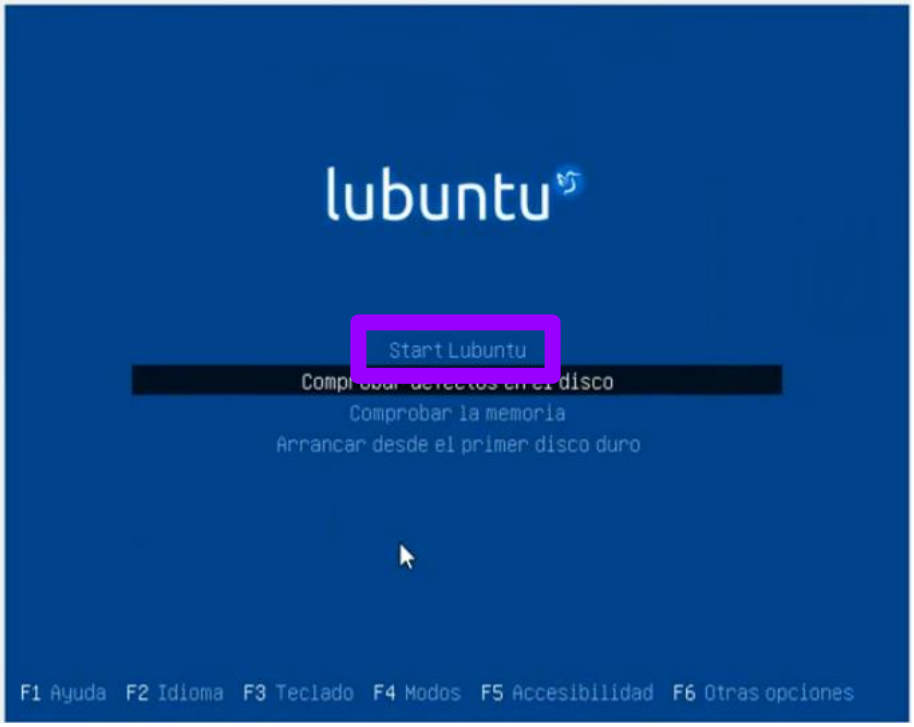
6. Aparecerá la siguiente ventana a manera de resumen de las configuraciones de la máquina virtual Lubuntu, seguidamente se da clic en el botón *Terminar*.



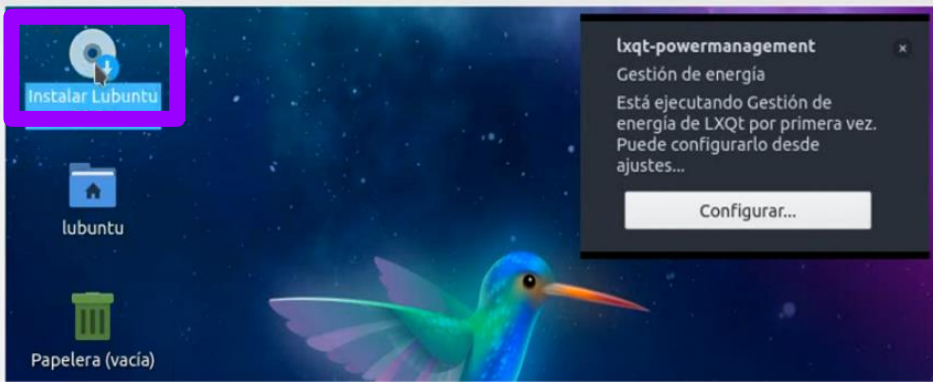
7. Se escoge el idioma para las instrucciones de instalación y damos *Enter*.



8. Aparecerá la siguiente ventana en la se escoge la opción *Start Lubuntu.*



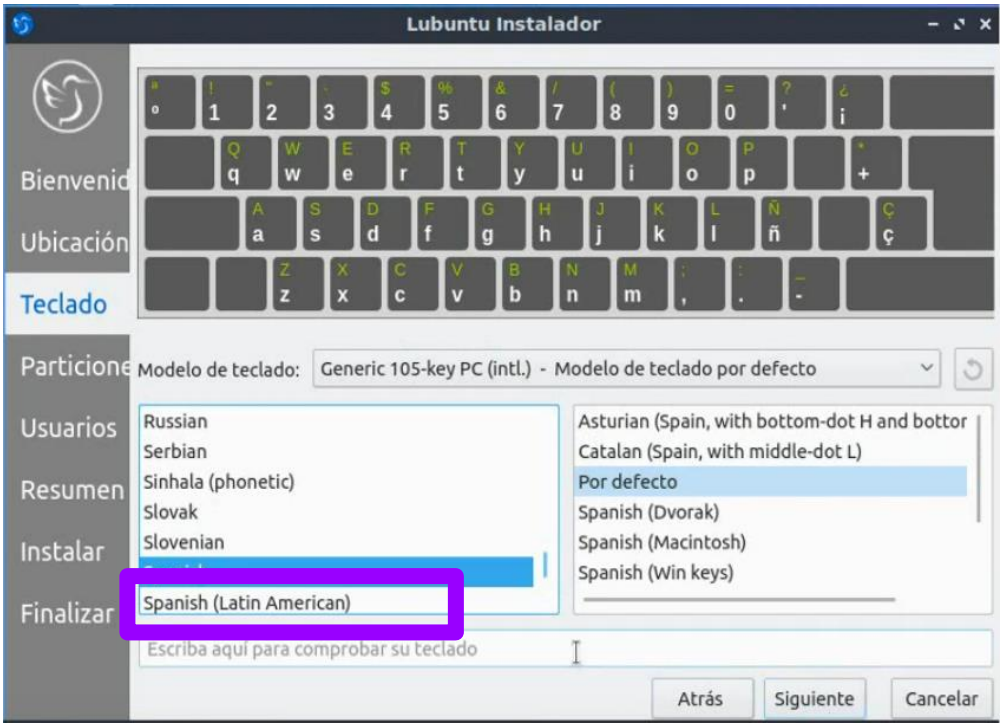
9. Se hace doble clic sobre el ícono de disco que lleva por nombre *Instalar Lubuntu 22.04.2*.



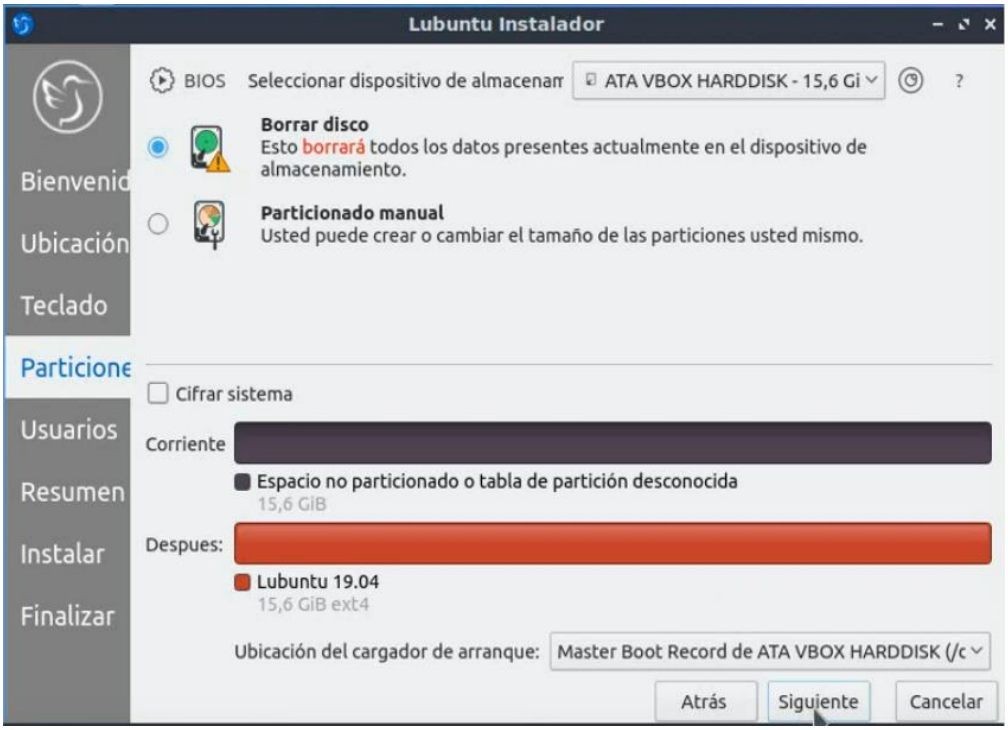
10. Aparece la pantalla del instalador, en caso de ser necesario se escoge el idioma y luego se da clic al botón *Siguiente.*

    Como siguiente paso se selecciona la ubicación y también se hace clic sobre el botón *Siguiente.*

11. Se selecciona el teclado en idioma español (Latinoamericano) para evitar tener inconvenientes al momento de utilizar el mencionado. Se hace clic sobre el botón *Siguiente.*

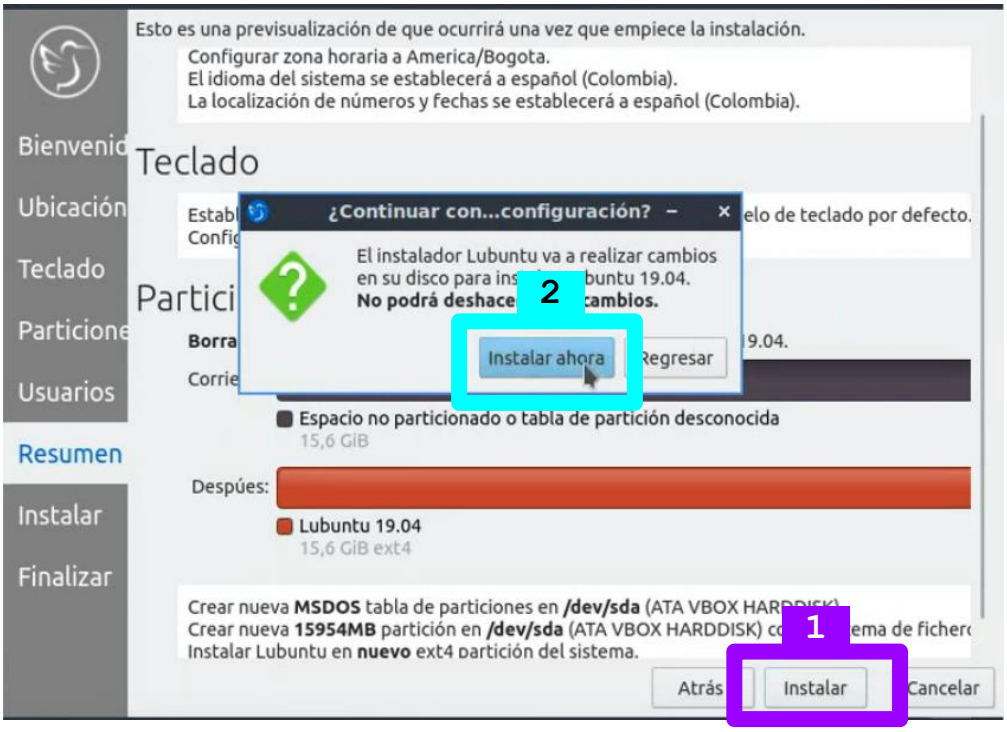


12. En la ventana que aparece después del paso anterior, se debe seleccionar la opción *Borrar disco* y hacer clic sobre el botón *Siguiente.*



13. Se asigna las credenciales de acceso a nuestra máquina virtual Lubuntu y se da clic en el botón *Siguiente*.

14. A continuación, se mostrará una ventana a manera de resumen de las configuraciones hechas, se hace clic sobre el botón *Instalar* y, aparecerá un pequeño alert o modal en el que se hace clic sobre el botón *Instalar ahora*.



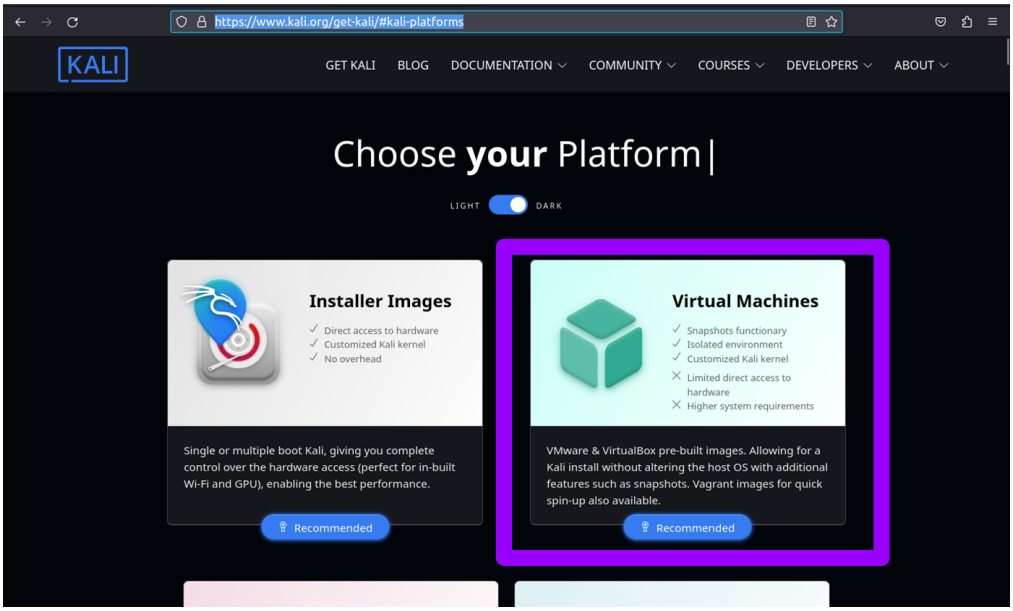
15. Esta ventana nos indica que la instalación está en curso.

16. Cuando termina el proceso de instalación, la ventana que se muestra es la siguiente, misma en la que se hace clic sobre el botón *Hecho* para reiniciar la máquina virtual y con ello se la tiene en el entorno de VirtualBox.

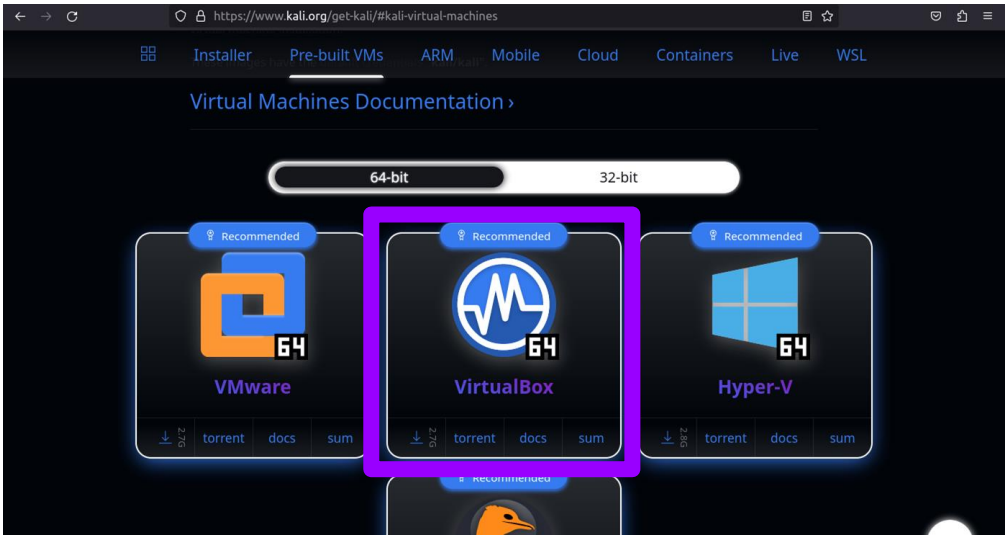
ANEXO B

Instalación de la máquina virtual Kali Linux

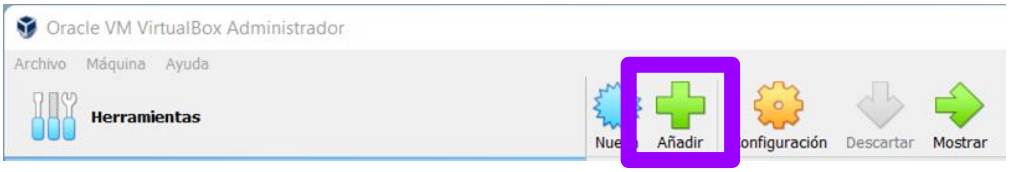
1. Se accede a la página oficial de Kali Linux (https://www.kali.org/get-kali/#kali-platforms) para descargar la imagen ISO adaptada a entornos virtuales.



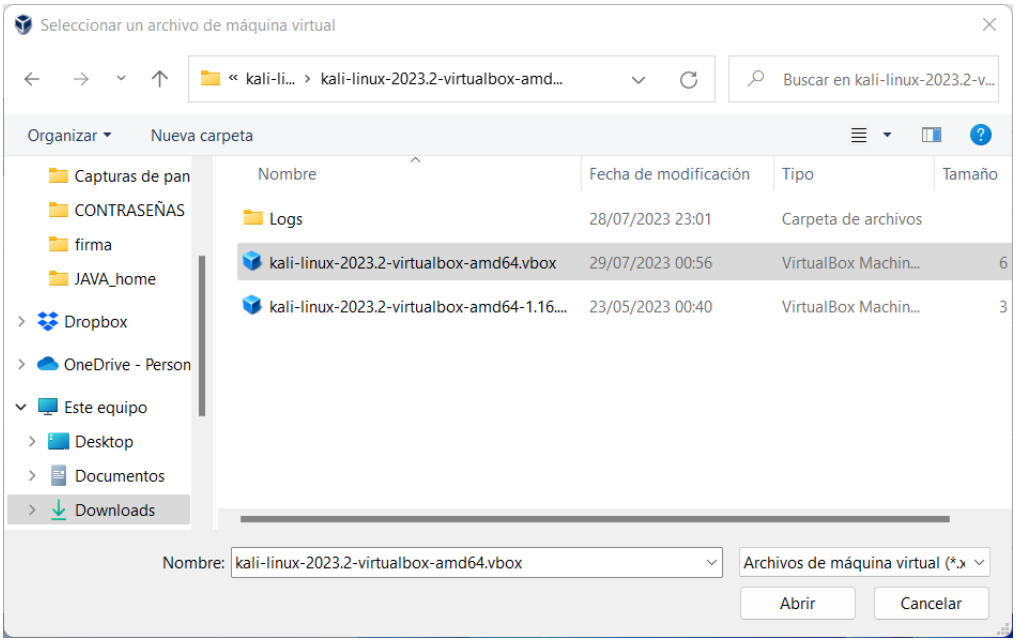
2. En vista que el entorno en el que este proyecto es realizado es VirtualBox, se selecciona esa opción.



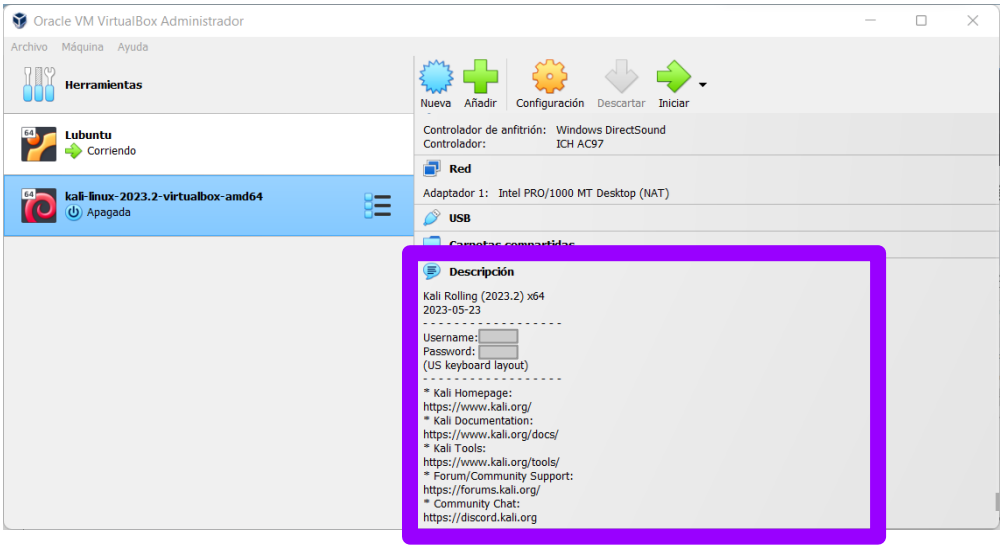
3. Teniendo la imagen ISO descargada se procede a abrir VirtualBox y hacer clic sobre la opción *Añadir*.



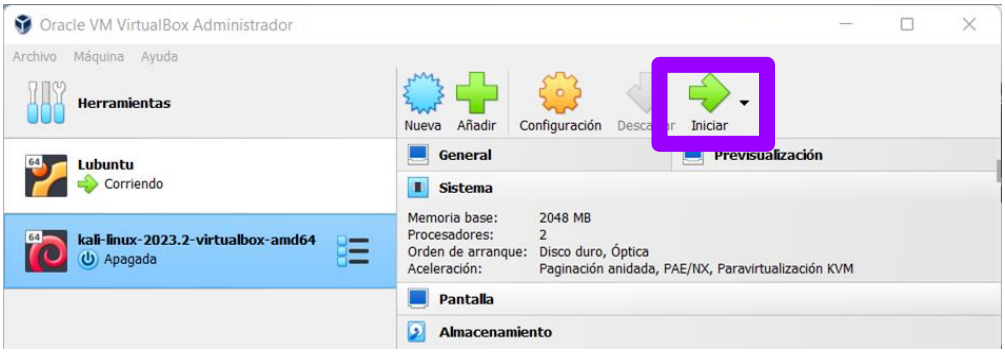
4. Se mostrará una ventana semejante a la que se encuentra a continuación, en la que se escoge el archivo .vbox (en caso se haya descomprimido el archivo descargado de Kali Linux para entornos virtuales)



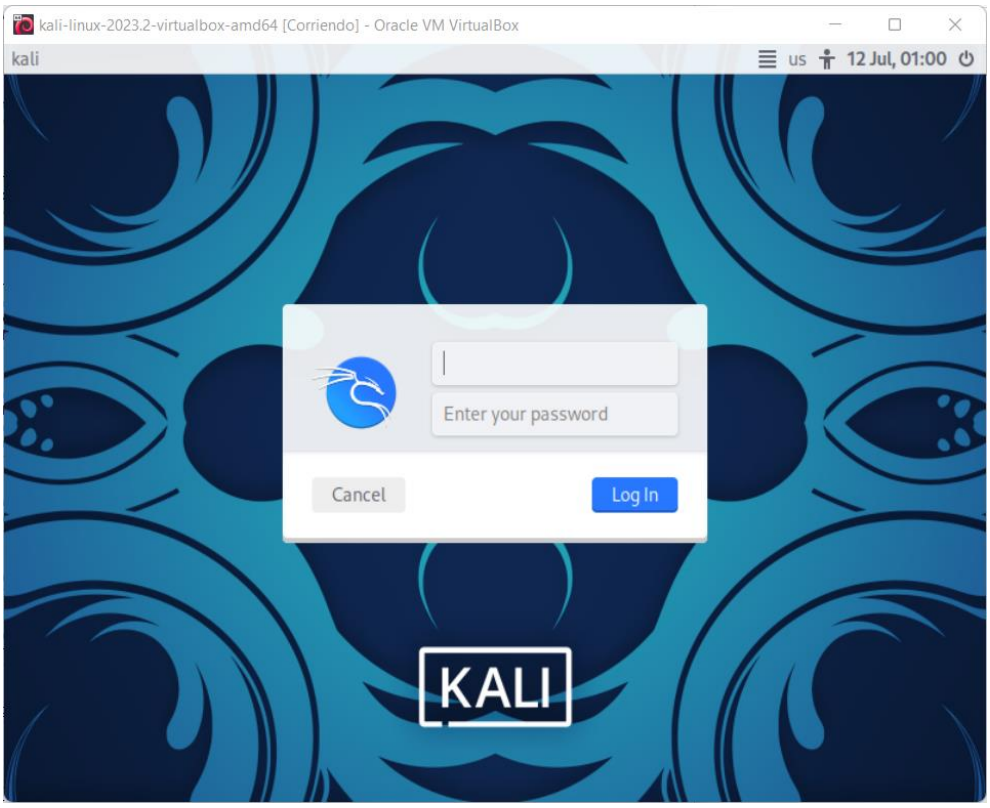
5. Y con ese paso se tiene Kali Linux en VirtualBox, las credenciales de acceso y configuraciones de la máquina virtual vienen establecidas por defecto y se pueden ver al hacer clic sobre el nombre de la máquina virtual, en el apartado *Descripción*.



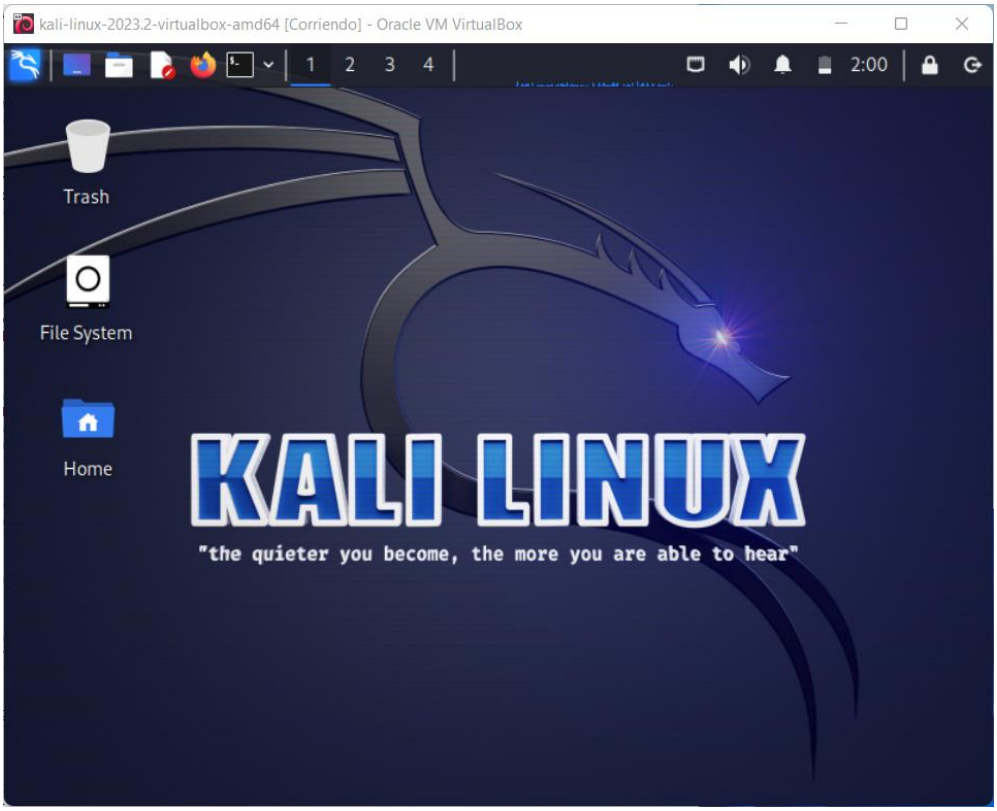
6. Para cerciorarse de que la máquina virtual funciona, hacemos clic sobre el nombre de la máquina virtual y luego otro clic en la opción *Iniciar*.



7. A continuación, se verá la pantalla de Kali Linux pidiendo las credenciales de usuario para poder utilizar la máquina virtual, se colocan las mismas que aparecen en la figura del paso N°5.



8. Al ingresar las credenciales de forma correcta se debería tener una vista semejante a la siguiente figura:



9. Con eso comprobamos que la máquina virtual Kali Linux se añadió correctamente a VirtualBox.

ANEXO C

Políticas cargadas en el inicio de sesión

```
# Este script registra qué scripts se cargaron durante cada ejecución.
@load misc/loaded-scripts

# Aplica los scripts de ajuste por defecto para los ajustes comunes.
@load tuning/defaults

# Estimación y registro de la pérdida de capturas.
@load misc/capture-loss

# Activa el registro de estadísticas de memoria, paquetes y retrasos.
@load misc/stats

# Cargue el script de detección de escaneos.  Está desactivado por defecto
# porque a menudo causa problemas de rendimiento.
@load misc/scan

# Detectar traceroute ejecutándose en la red. Esto podría causar
# problemas de rendimiento cuando hay muchos traceroutes en su red.
# Activar con precaución.
@load misc/detect-traceroute
```

```
# Generar avisos cuando se descubran versiones vulnerables de software.
# Por defecto sólo se monitoriza el software encontrado en el espacio de
# direcciones definido como "local".  Consulte la documentación del marco de
# software para más información.
@load frameworks/software/vulnerable

# Detectar el cambio de software (por ejemplo, si un atacante instala un
# SSHD pirateado)
@load frameworks/software/version-changes

# Esto añade firmas para detectar shells de ventanas de texto claro hacia
# adelante y hacia atrás.
@load-sigs frameworks/signatures/detect-windows-shells

# Carga todos los scripts que detecta software en varios protocolos.
@load protocols/ftp/software
@load protocols/smtp/software
@load protocols/ssh/software
@load protocols/http/software

# El script detect-webapps posiblemente podría causar problemas de rendimiento
#cuando se ejecuta en el tráfico en vivo.  Habilítelo con precaución.
@load protocols/http/detect-webapps

# Este script detecta los resultados DNS que apuntan hacia su site::local_nets
# donde el nombre no es parte de su zona DNS local y está siendo alojado
# externamente.  Requiere que la variable site::local_zones esté definida.
@load protocols/dns/detect-external-names

# Script para detectar diversas actividades en sesiones FTP.
@load protocols/ftp/detect

# Scripts que hacen seguimiento de activos.
@load protocols/conn/known-hosts
@load protocols/conn/known-services
@load protocols/ssl/known-certs

# Habilita la validación de certificados SSL/TLS.
@load protocols/ssl/validate-certs

# Evita el registro de certificados SSL CA en x509.log
@load protocols/ssl/log-hostcerts-only

# Si tiene soporte GeoIP incorporado, haga algunas detecciones geográficas y
# registro del tráfico SSH.
@load protocols/ssh/geo-data
# Detectar hosts que realizan ataques de fuerza bruta SSH.
@load protocols/ssh/detect-bruteforcing
# Detectar inicios de sesión con nombres de host "interesantes".
@load protocols/ssh/interesting-hostnames

# Detecta ataques de inyección SQL.
@load protocols/http/detect-sqli
```

```
#### Gestión de archivos de red  ####

# Activa el hash MD5 y SHA1 para todos los archivos.
@load frameworks/files/hash-all-files

# Detectar sumas SHA1 en el Registro Hash de Malware de Team Cymru.
@load frameworks/files/detect-MHR

# Ampliar las alertas por correo electrónico para incluir nombres de host
@load policy/frameworks/notice/extend-email/hostnames

# Descomente la siguiente línea para activar la detección del ataque heartbleed.
# Esto puede afectar un poco al rendimiento.
@load policy/protocols/ssl/heartbleed

# Descomente la siguiente línea para habilitar el registro de las VLAN de
# conexión. Esto añade dos campos VLAN al archivo conn.log.
@load policy/protocols/conn/vlan-logging

# Descomente la siguiente línea para habilitar el registro de direcciones de
# capa de enlace. Activando esto se añade la dirección de capa de enlace para
# cada punto final de conexión al archivo conn.log.
@load policy/protocols/conn/mac-logging

# Descomenta esto para obtener el estado del paquete zkg.
# @load packages
```

ANEXO D

Zeek scripts

```
/opt/zeek/share/zeek/base/init-bare.zeek
       /opt/zeek/share/zeek/base/bif/const.bif.zeek
       /opt/zeek/share/zeek/base/bif/types.bif.zeek
       /opt/zeek/share/zeek/base/bif/zeek.bif.zeek
       /opt/zeek/share/zeek/base/bif/stats.bif.zeek
       /opt/zeek/share/zeek/base/bif/reporter.bif.zeek
       /opt/zeek/share/zeek/base/bif/strings.bif.zeek
       /opt/zeek/share/zeek/base/bif/option.bif.zeek
       /opt/zeek/share/zeek/base/frameworks/supervisor/api.zeek
       /opt/zeek/share/zeek/base/bif/supervisor.bif.zeek
       /opt/zeek/share/zeek/base/bif/packet_analysis.bif.zeek
       /opt/zeek/share/zeek/base/bif/CPP-load.bif.zeek
       /opt/zeek/share/zeek/base/bif/plugins/Zeek_SNMP.types.bif.zeek
       /opt/zeek/share/zeek/base/bif/plugins/Zeek_KRB.types.bif.zeek
       /opt/zeek/share/zeek/base/bif/event.bif.zeek
       /opt/zeek/share/zeek/base/packet-protocols/__load__.zeek
       /opt/zeek/share/zeek/base/packet-protocols/main.zeek
       /opt/zeek/share/zeek/base/frameworks/analyzer/main.zeek
       /opt/zeek/share/zeek/base/frameworks/packet-filter/utils.zeek
      /opt/zeek/share/zeek/base/bif/analyzer.bif.zeek
       /opt/zeek/share/zeek/base/packet-protocols/root/__load__.zeek
       /opt/zeek/share/zeek/base/packet-protocols/root/main.zeek
       /opt/zeek/share/zeek/base/packet-protocols/ip/__load__.zeek
       /opt/zeek/share/zeek/base/packet-protocols/ip/main.zeek
```

```
    /opt/zeek/share/zeek/base/packet-protocols/skip/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/skip/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ethernet/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ethernet/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/fddi/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/fddi/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ieee802_11/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ieee802_11/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ieee802_11_radio/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ieee802_11_radio/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/linux_sll/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/linux_sll/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/nflog/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/nflog/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/null/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/null/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ppp_serial/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ppp_serial/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/pppoe/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/pppoe/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/vlan/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/vlan/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/mpls/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/mpls/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/vntag/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/vntag/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/udp/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/udp/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/tcp/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/tcp/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/icmp/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/icmp/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/gre/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/gre/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/iptunnel/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/iptunnel/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ayiya/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/ayiya/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/geneve/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/geneve/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/vxlan/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/vxlan/main.zeek
    /opt/zeek/share/zeek/base/packet-protocols/teredo/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/teredo/main.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_Teredo.functions.bif.zeek
    /opt/zeek/share/zeek/base/packet-protocols/gtpv1/__load__.zeek
    /opt/zeek/share/zeek/base/packet-protocols/gtpv1/main.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_GTPv1.functions.bif.zeek
/opt/zeek/share/zeek/base/init-frameworks-and-bifs.zeek
    /opt/zeek/share/zeek/base/frameworks/logging/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/logging/main.zeek
    /opt/zeek/share/zeek/base/bif/logging.bif.zeek
    /opt/zeek/share/zeek/base/frameworks/logging/postprocessors/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/logging/postprocessors/scp.zeek
    /opt/zeek/share/zeek/base/frameworks/logging/postprocessors/sftp.zeek
```

```
/opt/zeek/share/zeek/base/frameworks/logging/writers/ascii.zeek
/opt/zeek/share/zeek/base/frameworks/logging/writers/sqlite.zeek
/opt/zeek/share/zeek/base/frameworks/logging/writers/none.zeek
/opt/zeek/share/zeek/base/frameworks/broker/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/broker/main.zeek
/opt/zeek/share/zeek/base/bif/comm.bif.zeek
/opt/zeek/share/zeek/base/bif/messaging.bif.zeek
/opt/zeek/share/zeek/base/frameworks/broker/store.zeek
/opt/zeek/share/zeek/base/bif/data.bif.zeek
/opt/zeek/share/zeek/base/bif/store.bif.zeek
/opt/zeek/share/zeek/base/frameworks/broker/log.zeek
/opt/zeek/share/zeek/base/frameworks/supervisor/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/supervisor/control.zeek
/opt/zeek/share/zeek/base/frameworks/supervisor/main.zeek
/opt/zeek/share/zeek/base/frameworks/input/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/input/main.zeek
/opt/zeek/share/zeek/base/bif/input.bif.zeek
/opt/zeek/share/zeek/base/frameworks/input/readers/ascii.zeek
/opt/zeek/share/zeek/base/frameworks/input/readers/raw.zeek
/opt/zeek/share/zeek/base/frameworks/input/readers/benchmark.zeek
/opt/zeek/share/zeek/base/frameworks/input/readers/binary.zeek
/opt/zeek/share/zeek/base/frameworks/input/readers/config.zeek
/opt/zeek/share/zeek/base/frameworks/input/readers/sqlite.zeek
/opt/zeek/share/zeek/base/frameworks/analyzer/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/files/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/files/main.zeek
/opt/zeek/share/zeek/base/bif/file_analysis.bif.zeek
/opt/zeek/share/zeek/base/utils/site.zeek
/opt/zeek/share/zeek/base/utils/patterns.zeek
/opt/zeek/share/zeek/base/frameworks/files/magic/__load__.zeek
/opt/zeek/share/zeek/base/bif/__load__.zeek
/opt/zeek/share/zeek/base/bif/telemetry.bif.zeek
/opt/zeek/share/zeek/base/bif/zeekygen.bif.zeek
/opt/zeek/share/zeek/base/bif/pcap.bif.zeek
/opt/zeek/share/zeek/base/bif/bloom-filter.bif.zeek
/opt/zeek/share/zeek/base/bif/cardinality-counter.bif.zeek
/opt/zeek/share/zeek/base/bif/top-k.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/__load__.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_BitTorrent.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_ConnSize.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_ConnSize.functions.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_DCE_RPC.consts.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_DCE_RPC.types.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_DCE_RPC.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_DHCP.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_DHCP.types.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_DNP3.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_DNS.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_File.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_Finger.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_FTP.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_FTP.functions.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_Gnutella.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_GSSAPI.events.bif.zeek
/opt/zeek/share/zeek/base/bif/plugins/Zeek_HTTP.events.bif.zeek
```

```
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_HTTP.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Ident.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_IMAP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_IRC.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_KRB.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Login.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Login.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_MIME.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Modbus.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_MQTT.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_MQTT.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_MySQL.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NCP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NCP.consts.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NetBIOS.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NetBIOS.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NTLM.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NTLM.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NTP.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_NTP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_POP3.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_RADIUS.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_RDP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_RDP.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_RFB.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_RPC.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SIP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_check_directory.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_close.bif.zeek

        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_create_directory.bif.zee
k
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_echo.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_logoff_andx.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_negotiate.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_nt_create_andx.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_nt_cancel.bif.zeek

        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_query_information.bif.ze
ek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_read_andx.bif.zeek

        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_session_setup_andx.bif.z
eek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_transaction.bif.zeek

        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_transaction_secondary.bi
f.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_transaction2.bif.zeek

        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_transaction2_secondary.b
if.zeek

        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_tree_connect_andx.bif.ze
ek
```

```
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_tree_disconnect.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_com_write_andx.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb1_events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_close.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_create.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_negotiate.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_read.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_session_setup.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_set_info.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_tree_connect.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_tree_disconnect.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_write.bif.zeek

        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_com_transform_header.bif.zee
k
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.smb2_events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.consts.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMB.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMTP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SMTP.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SNMP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SOCKS.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SSH.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SSH.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SSL.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SSL.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SSL.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_SSL.consts.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Syslog.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_TCP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_TCP.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_TCP.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_XMPP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_ARP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_UDP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_ICMP.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Geneve.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_VXLAN.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Teredo.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_GTPv1.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_FileEntropy.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_FileExtract.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_FileExtract.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_FileHash.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_PE.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Unified2.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_Unified2.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_X509.events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_X509.types.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_X509.functions.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_X509.ocsp_events.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_AsciiReader.ascii.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_BenchmarkReader.benchmark.bif.zeek
        /opt/zeek/share/zeek/base/bif/plugins/Zeek_BinaryReader.binary.bif.zeek
```

```
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_ConfigReader.config.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_RawReader.raw.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_SQLiteReader.sqlite.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_AsciiWriter.ascii.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_NoneWriter.none.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_SQLiteWriter.sqlite.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_Spicy.consts.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_Spicy.events.bif.zeek
    /opt/zeek/share/zeek/base/bif/plugins/Zeek_Spicy.functions.bif.zeek
/opt/zeek/share/zeek/base/init-default.zeek
    /opt/zeek/share/zeek/base/utils/active-http.zeek
    /opt/zeek/share/zeek/base/utils/exec.zeek
    /opt/zeek/share/zeek/base/utils/addrs.zeek
    /opt/zeek/share/zeek/base/utils/backtrace.zeek
    /opt/zeek/share/zeek/base/utils/conn-ids.zeek
    /opt/zeek/share/zeek/base/utils/dir.zeek
    /opt/zeek/share/zeek/base/frameworks/reporter/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/reporter/main.zeek
    /opt/zeek/share/zeek/base/utils/paths.zeek
    /opt/zeek/share/zeek/base/utils/directions-and-hosts.zeek
    /opt/zeek/share/zeek/base/utils/email.zeek
    /opt/zeek/share/zeek/base/utils/files.zeek
    /opt/zeek/share/zeek/base/utils/geoip-distance.zeek
    /opt/zeek/share/zeek/base/utils/hash_hrw.zeek
    /opt/zeek/share/zeek/base/utils/numbers.zeek
    /opt/zeek/share/zeek/base/utils/queue.zeek
    /opt/zeek/share/zeek/base/utils/strings.zeek
    /opt/zeek/share/zeek/base/utils/thresholds.zeek
    /opt/zeek/share/zeek/base/utils/time.zeek
    /opt/zeek/share/zeek/base/utils/urls.zeek
    /opt/zeek/share/zeek/base/frameworks/notice/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/notice/main.zeek
    /opt/zeek/share/zeek/base/frameworks/cluster/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/cluster/main.zeek
           /opt/zeek/share/zeek/base/frameworks/control/__load__.zeek
           /opt/zeek/share/zeek/base/frameworks/control/main.zeek
    /opt/zeek/share/zeek/base/frameworks/cluster/pools.zeek
    /opt/zeek/share/zeek/base/frameworks/notice/weird.zeek
    /opt/zeek/share/zeek/base/frameworks/notice/actions/email_admin.zeek
    /opt/zeek/share/zeek/base/frameworks/notice/actions/page.zeek
    /opt/zeek/share/zeek/base/frameworks/notice/actions/add-geodata.zeek
    /opt/zeek/share/zeek/base/frameworks/notice/actions/pp-alarms.zeek
    /opt/zeek/share/zeek/base/frameworks/dpd/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/dpd/main.zeek
    /opt/zeek/share/zeek/base/frameworks/signatures/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/signatures/main.zeek
    /opt/zeek/share/zeek/base/frameworks/packet-filter/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/packet-filter/main.zeek
    /opt/zeek/share/zeek/base/frameworks/packet-filter/netstats.zeek
    /opt/zeek/share/zeek/base/frameworks/software/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/software/main.zeek
    /opt/zeek/share/zeek/base/frameworks/intel/__load__.zeek
    /opt/zeek/share/zeek/base/frameworks/intel/main.zeek
    /opt/zeek/share/zeek/base/frameworks/intel/files.zeek
    /opt/zeek/share/zeek/base/frameworks/intel/input.zeek
```

```
/opt/zeek/share/zeek/base/frameworks/config/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/config/main.zeek
/opt/zeek/share/zeek/base/frameworks/config/input.zeek
/opt/zeek/share/zeek/base/frameworks/config/weird.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/main.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/average.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/hll_unique.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/last.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/max.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/min.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/sample.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/std-dev.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/variance.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/sum.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/topk.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/plugins/unique.zeek
/opt/zeek/share/zeek/base/frameworks/sumstats/non-cluster.zeek
/opt/zeek/share/zeek/base/frameworks/tunnels/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/tunnels/main.zeek
/opt/zeek/share/zeek/base/protocols/conn/removal-hooks.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/consts.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/types.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/main.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/plugins/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/plugins/ryu.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/plugins/log.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/plugins/broker.zeek
/opt/zeek/share/zeek/base/frameworks/openflow/non-cluster.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/types.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/main.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/plugin.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/plugins/__load__.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/plugins/debug.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/plugins/openflow.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/plugins/packetfilter.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/plugins/broker.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/plugins/acld.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/drop.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/shunt.zeek
/opt/zeek/share/zeek/base/frameworks/netcontrol/non-cluster.zeek
/opt/zeek/share/zeek/base/protocols/conn/__load__.zeek
/opt/zeek/share/zeek/base/protocols/conn/main.zeek
/opt/zeek/share/zeek/base/protocols/conn/contents.zeek
/opt/zeek/share/zeek/base/protocols/conn/inactivity.zeek
/opt/zeek/share/zeek/base/protocols/conn/polling.zeek
/opt/zeek/share/zeek/base/protocols/conn/thresholds.zeek
/opt/zeek/share/zeek/base/protocols/dce-rpc/__load__.zeek
/opt/zeek/share/zeek/base/protocols/dce-rpc/consts.zeek
/opt/zeek/share/zeek/base/protocols/dce-rpc/main.zeek
/opt/zeek/share/zeek/base/protocols/dhcp/__load__.zeek
/opt/zeek/share/zeek/base/protocols/dhcp/consts.zeek
```

```
/opt/zeek/share/zeek/base/protocols/dhcp/main.zeek
/opt/zeek/share/zeek/base/protocols/dnp3/__load__.zeek
/opt/zeek/share/zeek/base/protocols/dnp3/main.zeek
/opt/zeek/share/zeek/base/protocols/dnp3/consts.zeek
/opt/zeek/share/zeek/base/protocols/dns/__load__.zeek
/opt/zeek/share/zeek/base/protocols/dns/consts.zeek
/opt/zeek/share/zeek/base/protocols/dns/main.zeek
/opt/zeek/share/zeek/base/protocols/ftp/__load__.zeek
/opt/zeek/share/zeek/base/protocols/ftp/utils-commands.zeek
/opt/zeek/share/zeek/base/protocols/ftp/info.zeek
/opt/zeek/share/zeek/base/protocols/ftp/main.zeek
/opt/zeek/share/zeek/base/protocols/ftp/utils.zeek
/opt/zeek/share/zeek/base/protocols/ftp/files.zeek
/opt/zeek/share/zeek/base/protocols/ftp/gridftp.zeek
/opt/zeek/share/zeek/base/protocols/ssl/__load__.zeek
/opt/zeek/share/zeek/base/protocols/ssl/consts.zeek
/opt/zeek/share/zeek/base/protocols/ssl/main.zeek
/opt/zeek/share/zeek/base/protocols/ssl/mozilla-ca-list.zeek
/opt/zeek/share/zeek/base/protocols/ssl/ct-list.zeek
/opt/zeek/share/zeek/base/protocols/ssl/files.zeek
       /opt/zeek/share/zeek/base/files/x509/__load__.zeek
       /opt/zeek/share/zeek/base/files/x509/main.zeek
       /opt/zeek/share/zeek/base/files/hash/__load__.zeek
              /opt/zeek/share/zeek/base/files/hash/main.zeek
       /opt/zeek/share/zeek/base/files/x509/certificate-event-cache.zeek
       /opt/zeek/share/zeek/base/files/x509/log-ocsp.zeek
/opt/zeek/share/zeek/base/protocols/http/__load__.zeek
/opt/zeek/share/zeek/base/protocols/http/main.zeek
/opt/zeek/share/zeek/base/protocols/http/entities.zeek
/opt/zeek/share/zeek/base/protocols/http/utils.zeek
/opt/zeek/share/zeek/base/protocols/http/files.zeek
/opt/zeek/share/zeek/base/protocols/imap/__load__.zeek
/opt/zeek/share/zeek/base/protocols/imap/main.zeek
/opt/zeek/share/zeek/base/protocols/irc/__load__.zeek
/opt/zeek/share/zeek/base/protocols/irc/main.zeek
/opt/zeek/share/zeek/base/protocols/irc/dcc-send.zeek
/opt/zeek/share/zeek/base/protocols/irc/files.zeek
/opt/zeek/share/zeek/base/protocols/krb/__load__.zeek
/opt/zeek/share/zeek/base/protocols/krb/main.zeek
/opt/zeek/share/zeek/base/protocols/krb/consts.zeek
/opt/zeek/share/zeek/base/protocols/krb/files.zeek
/opt/zeek/share/zeek/base/protocols/modbus/__load__.zeek
/opt/zeek/share/zeek/base/protocols/modbus/consts.zeek
/opt/zeek/share/zeek/base/protocols/modbus/main.zeek
/opt/zeek/share/zeek/base/protocols/mqtt/__load__.zeek
/opt/zeek/share/zeek/base/protocols/mqtt/consts.zeek
/opt/zeek/share/zeek/base/protocols/mysql/__load__.zeek
/opt/zeek/share/zeek/base/protocols/mysql/main.zeek
/opt/zeek/share/zeek/base/protocols/mysql/consts.zeek
/opt/zeek/share/zeek/base/protocols/ntlm/__load__.zeek
/opt/zeek/share/zeek/base/protocols/ntlm/main.zeek
/opt/zeek/share/zeek/base/protocols/ntp/__load__.zeek
/opt/zeek/share/zeek/base/protocols/ntp/main.zeek
/opt/zeek/share/zeek/base/protocols/ntp/consts.zeek
/opt/zeek/share/zeek/base/protocols/pop3/__load__.zeek
```

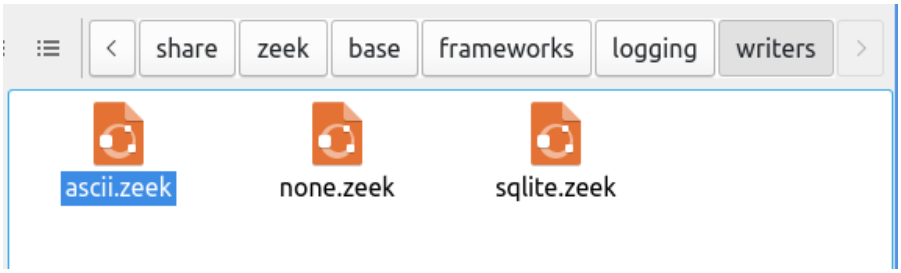
```
    /opt/zeek/share/zeek/base/protocols/radius/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/radius/main.zeek
    /opt/zeek/share/zeek/base/protocols/radius/consts.zeek
    /opt/zeek/share/zeek/base/protocols/rdp/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/rdp/consts.zeek
    /opt/zeek/share/zeek/base/protocols/rdp/main.zeek
    /opt/zeek/share/zeek/base/protocols/rfb/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/rfb/main.zeek
    /opt/zeek/share/zeek/base/protocols/sip/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/sip/main.zeek
    /opt/zeek/share/zeek/base/protocols/snmp/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/snmp/main.zeek
    /opt/zeek/share/zeek/base/protocols/smb/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/smb/consts.zeek
    /opt/zeek/share/zeek/base/protocols/smb/const-dos-error.zeek
    /opt/zeek/share/zeek/base/protocols/smb/const-nt-status.zeek
    /opt/zeek/share/zeek/base/protocols/smb/main.zeek
    /opt/zeek/share/zeek/base/protocols/smb/smb1-main.zeek
    /opt/zeek/share/zeek/base/protocols/smb/smb2-main.zeek
    /opt/zeek/share/zeek/base/protocols/smb/files.zeek
    /opt/zeek/share/zeek/base/protocols/smtp/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/smtp/main.zeek
    /opt/zeek/share/zeek/base/protocols/smtp/entities.zeek
    /opt/zeek/share/zeek/base/protocols/smtp/files.zeek
    /opt/zeek/share/zeek/base/protocols/socks/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/socks/consts.zeek
    /opt/zeek/share/zeek/base/protocols/socks/main.zeek
    /opt/zeek/share/zeek/base/protocols/ssh/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/ssh/main.zeek
    /opt/zeek/share/zeek/base/protocols/syslog/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/syslog/consts.zeek
    /opt/zeek/share/zeek/base/protocols/syslog/main.zeek
    /opt/zeek/share/zeek/base/protocols/tunnels/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/xmpp/__load__.zeek
    /opt/zeek/share/zeek/base/protocols/xmpp/main.zeek
    /opt/zeek/share/zeek/base/files/pe/__load__.zeek
    /opt/zeek/share/zeek/base/files/pe/consts.zeek
    /opt/zeek/share/zeek/base/files/pe/main.zeek
    /opt/zeek/share/zeek/base/files/extract/__load__.zeek
    /opt/zeek/share/zeek/base/files/extract/main.zeek
    /opt/zeek/share/zeek/base/misc/find-checksum-offloading.zeek
    /opt/zeek/share/zeek/base/misc/find-filtered-trace.zeek
    /opt/zeek/share/zeek/base/misc/installation.zeek
    /opt/zeek/share/zeek/base/misc/version.zeek
/opt/zeek/share/zeek/builtin-plugins/__preload__.zeek
    /opt/zeek/share/zeek/builtin-plugins/Zeek_Spicy/__preload__.zeek
/opt/zeek/share/zeek/builtin-plugins/__load__.zeek
    /opt/zeek/share/zeek/builtin-plugins/Zeek_Spicy/__load__.zeek
    /opt/zeek/share/zeek/builtin-plugins/Zeek_Spicy/Zeek/Spicy/bare.zeek
    /opt/zeek/share/zeek/builtin-plugins/Zeek_Spicy/Zeek/Spicy/default.zeek
/opt/zeek/spool/installed-scripts-do-not-touch/site/local.zeek
    /opt/zeek/share/zeek/policy/misc/loaded-scripts.zeek
    /opt/zeek/share/zeek/policy/tuning/defaults/__load__.zeek
    /opt/zeek/share/zeek/policy/tuning/defaults/packet-fragments.zeek
    /opt/zeek/share/zeek/policy/tuning/defaults/warnings.zeek
```

```
        /opt/zeek/share/zeek/policy/tuning/defaults/extracted_file_limits.zeek
        /opt/zeek/share/zeek/policy/misc/capture-loss.zeek
        /opt/zeek/share/zeek/policy/misc/stats.zeek
        /opt/zeek/share/zeek/policy/frameworks/software/vulnerable.zeek
        /opt/zeek/share/zeek/policy/frameworks/software/version-changes.zeek
        /opt/zeek/share/zeek/policy/protocols/ftp/software.zeek
        /opt/zeek/share/zeek/policy/protocols/smtp/software.zeek
        /opt/zeek/share/zeek/policy/protocols/ssh/software.zeek
        /opt/zeek/share/zeek/policy/protocols/http/software.zeek
        /opt/zeek/share/zeek/policy/protocols/dns/detect-external-names.zeek
        /opt/zeek/share/zeek/policy/protocols/ftp/detect.zeek
        /opt/zeek/share/zeek/policy/protocols/conn/known-hosts.zeek
        /opt/zeek/share/zeek/policy/protocols/conn/known-services.zeek
        /opt/zeek/share/zeek/policy/protocols/ssl/known-certs.zeek
        /opt/zeek/share/zeek/policy/protocols/ssl/validate-certs.zeek
        /opt/zeek/share/zeek/policy/protocols/ssl/log-hostcerts-only.zeek
        /opt/zeek/share/zeek/policy/protocols/ssh/geo-data.zeek
        /opt/zeek/share/zeek/policy/protocols/ssh/detect-bruteforcing.zeek
        /opt/zeek/share/zeek/policy/protocols/ssh/interesting-hostnames.zeek
        /opt/zeek/share/zeek/policy/protocols/http/detect-sqli.zeek
        /opt/zeek/share/zeek/policy/frameworks/files/hash-all-files.zeek
        /opt/zeek/share/zeek/policy/frameworks/files/detect-MHR.zeek
        /opt/zeek/share/zeek/policy/frameworks/notice/extend-email/hostnames.zeek
/opt/zeek/share/zeek/zeekctl/__load__.zeek
        /opt/zeek/share/zeek/zeekctl/main.zeek
        /opt/zeek/share/zeek/policy/frameworks/control/controllee.zeek
/opt/zeek/share/zeek/zeekctl/standalone.zeek
        /opt/zeek/spool/tmp/check-config-zeek/standalone-layout.zeek
        /opt/zeek/share/zeek/policy/misc/trim-trace-file.zeek
/opt/zeek/share/zeek/zeekctl/auto.zeek
        /opt/zeek/spool/tmp/check-config-zeek/local-networks.zeek
        /opt/zeek/spool/tmp/check-config-zeek/zeekctl-config.zeek
/opt/zeek/share/zeek/zeekctl/check.zeek
```

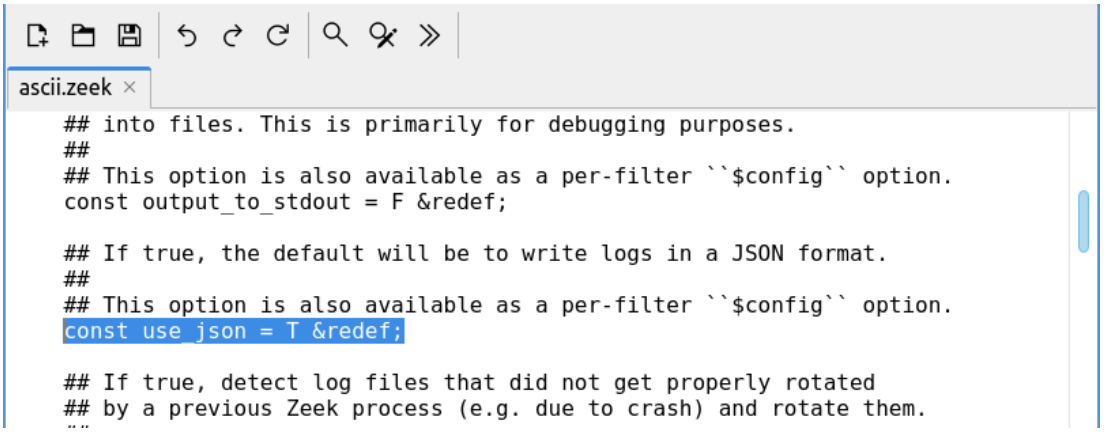
ANEXO E

Configuración de Zeek para generar reportes en formato JSON

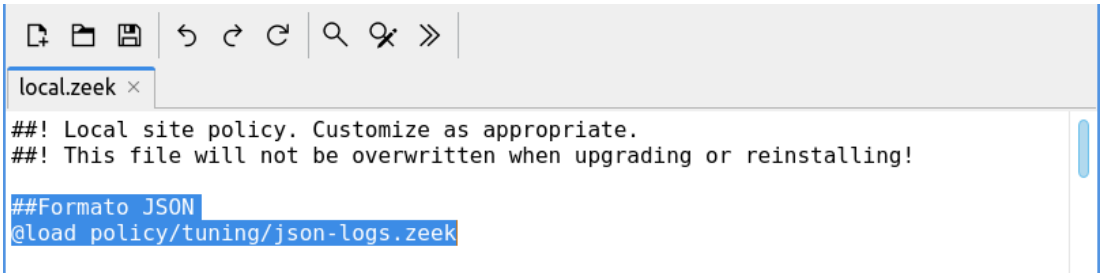
1. Dentro de la carpeta Zeek, ingresamos a: share/zeek/base/frameworks/logging/writers/ y en esa ubicación al archivo cuyo nombre es: *ascii.zeek.* Tal y como se muestra en la Figura…



2. Se cambia *const use_json = F &redef;* por *const use_json = T &redef;*. De tal forma que tenemos:



3. En el archivo *local.zeek* que se encuentra en la carpeta raíz de zeek, bajo la siguiente ruta: share/zeek/site/, añadimos la línea que se encuentra resaltada en la siguiente imagen:

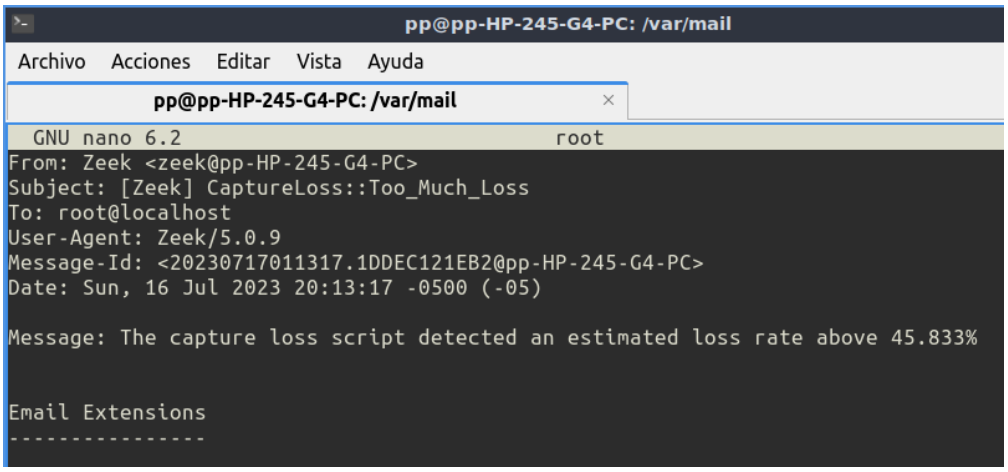


4. Volvemos a ejecutar Zeek Open Source.

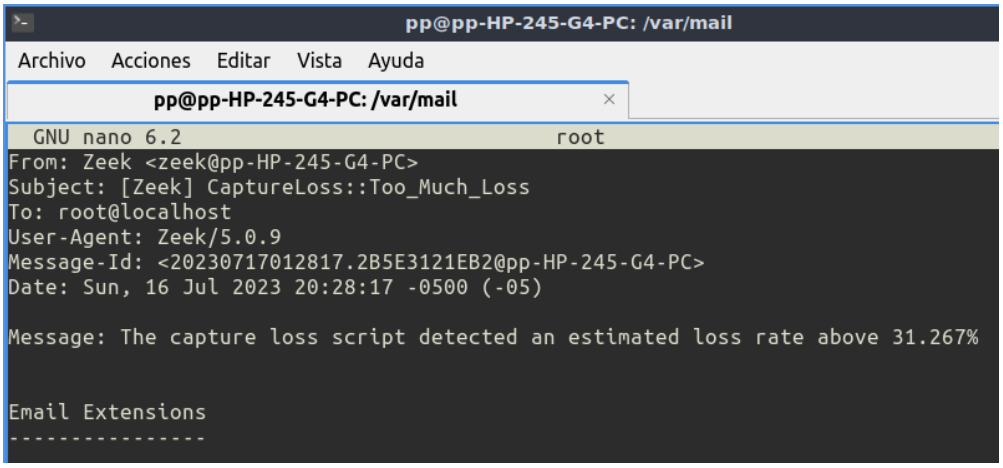
ANEXO F

Notificaciones de tipo CaptureLoss::Too_Much_Loss

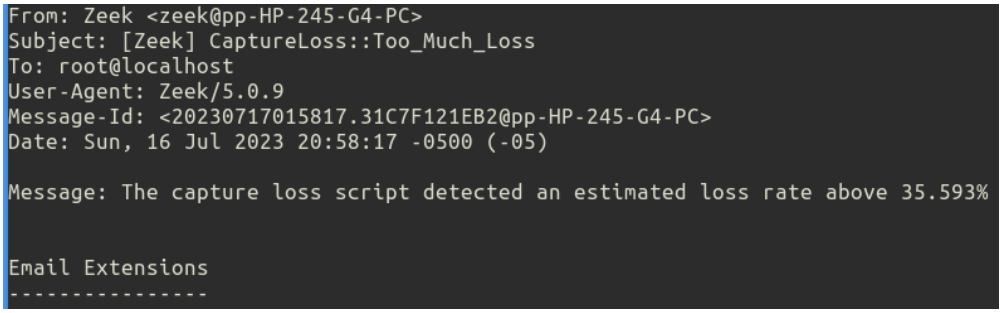
1. Pérdida detectada el día 16 de Julio a las 20:13:17 horas.



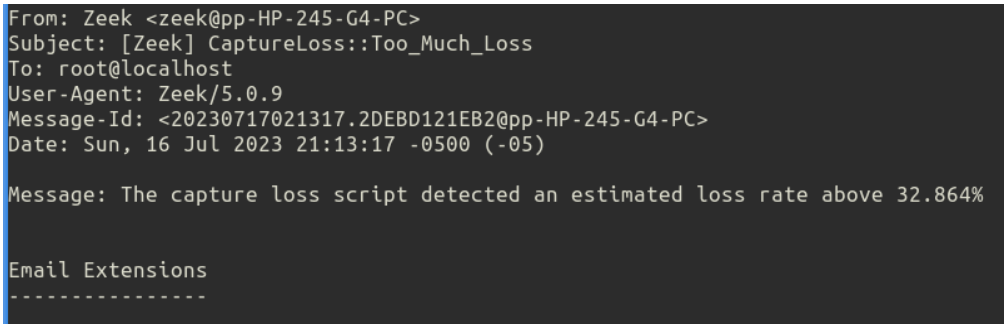
2. Pérdida detectada el día 16 de Julio a las 20:28:17 horas.



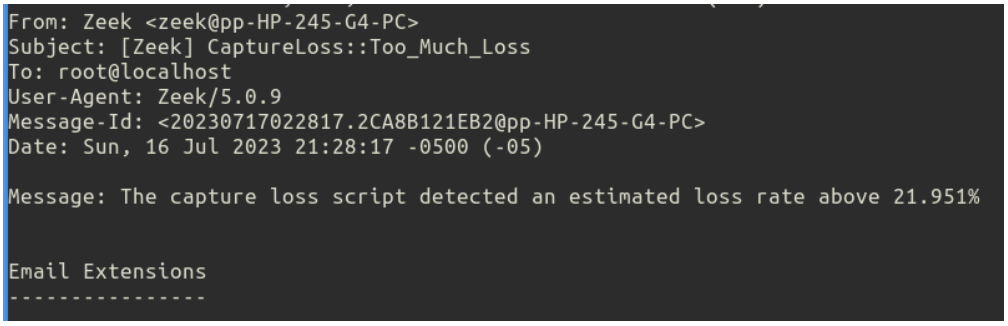
3. La tercera notificación de este tipo corresponde a la que se muestra en la Figura 27.
4. Pérdida detectada el día 16 de Julio a las 20:58:17 horas.



5. Pérdida detectada el día 16 de Julio a las 21:13:17 horas.



6. Pérdida detectada el día 16 de Julio a las 21:28:17 horas.



7. Pérdida detectada el día 16 de Julio a las 21:43:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717024317.28902121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 21:43:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 28.535%


Email Extensions
----------------
```

8. Pérdida detectada el día 16 de Julio a las 21:58:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717025817.2ED37121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 21:58:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 30.065%


Email Extensions
----------------
```

9. Pérdida detectada el día 16 de Julio a las 22:13:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717031317.1F490121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 22:13:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 26.016%


Email Extensions
----------------
```

10. Pérdida detectada el día 16 de Julio a las 22:28:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717032817.2232A121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 22:28:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 34.615%


Email Extensions
----------------
```

11. Pérdida detectada el día 16 de Julio a las 22:43:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717034317.2C3E0121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 22:43:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 29.577%


Email Extensions
----------------
```

12. Pérdida detectada el día 16 de Julio a las 22:58:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717035817.1D802121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 22:58:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 29.032%


Email Extensions
----------------
```

13. Pérdida detectada el día 16 de Julio a las 23:13:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717041317.1F447121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 23:13:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 26.117%


Email Extensions
----------------
```

14. Pérdida detectada el día 16 de Julio a las 23:28:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717042817.1D40B121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 23:28:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 18.298%


Email Extensions
----------------
```

15. Pérdida detectada el día 16 de Julio a las 23:43:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717044317.1E318121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 23:43:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 31.753%


Email Extensions
----------------
```

16. Pérdida detectada el día 16 de Julio a las 23:58:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717045817.1FB09121EB2@pp-HP-245-G4-PC>
Date: Sun, 16 Jul 2023 23:58:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 30.612%


Email Extensions
----------------
```

17. Pérdida detectada el día 17 de Julio a las 00:13:17 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717051317.1CA8F1236F6@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 00:13:17 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 66.594%


Email Extensions
----------------
```

18. Pérdida detectada el día 17 de Julio a las 00:28:27 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717052827.EA8021236F6@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 00:28:27 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.707%


Email Extensions
----------------
```

19. Pérdida detectada el día 17 de Julio a las 00:35:43 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717053543.4D4931236F1@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 00:35:43 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 25.134%


Email Extensions
----------------
```

20. Pérdida detectada el día 17 de Julio a las 17:27:29 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717222729.6C22E123729@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 17:27:29 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.000%


Email Extensions
----------------
```

21. Pérdida detectada el día 17 de Julio a las 17:42:29 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717224229.6EEC4123729@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 17:42:29 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 85.466%


Email Extensions
----------------
```

22. Pérdida detectada el día 17 de Julio a las 17:44:22 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717224803.6904D121E83@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 17:44:22 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 42.162%


Email Extensions
----------------
```

23. Pérdida detectada el día 17 de Julio a las 17:50:12 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230717225012.E9DAE1236F0@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 17:50:12 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 33.333%


Email Extensions
----------------
```

24. Pérdida detectada el día 17 de Julio a las 17:53:12 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230718021936.313E61236F5@pp-HP-245-G4-PC>
Date: Mon, 17 Jul 2023 17:53:59 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 30.769%


Email Extensions
----------------
```

25. Pérdida detectada el día 18 de Julio a las 19:45:20 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719004520.C7B3712372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 19:45:20 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 15.789%


Email Extensions
----------------
```

26. Pérdida detectada el día 18 de Julio a las 20:00:20 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719010020.BEADF12372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 20:00:20 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 80.462%


Email Extensions
----------------
```

27. Pérdida detectada el día 18 de Julio a las 20:15:20 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719011520.E7CFF12372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 20:15:20 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 44.241%


Email Extensions
----------------
```

28. Pérdida detectada el día 18 de Julio a las 20:30:20 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719013020.C967612372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 20:30:20 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 64.448%


Email Extensions
----------------
```

29. Pérdida detectada el día 18 de Julio a las 20:45:20 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719014520.C133D12372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 20:45:20 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 67.761%


Email Extensions
----------------
```

30. Pérdida detectada el día 18 de Julio a las 21:00:20 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719020020.E3D5512372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 21:00:20 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 66.859%


Email Extensions
----------------
```

31. Pérdida detectada el día 18 de Julio a las 21:20:20 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719022000.291EE123711@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 21:20:00 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 15.385%


Email Extensions
----------------
```

32. Pérdida detectada el día 18 de Julio a las 21:35:00 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719023500.1CC82123711@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 21:35:00 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 79.116%


Email Extensions
----------------
```

33. Pérdida detectada el día 19 de Julio a las 00:09:07 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719050907.5315812372F@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 00:09:07 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 44.136%


Email Extensions
----------------
```

34. Pérdida detectada el día 19 de Julio a las 00:24:07 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719052407.499F412372F@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 00:24:07 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.904%


Email Extensions
----------------
```

35. Pérdida detectada el día 19 de Julio a las 00:39:07 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719053907.5AACB12372F@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 00:39:07 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 15.789%


Email Extensions
----------------
```

36. Pérdida detectada el día 19 de Julio a las 00:50:38 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720011508.5D1AE121EA3@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 00:50:38 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 26.961%


Email Extensions
----------------
```

37. Pérdida detectada el día 19 de Julio a las 21:40:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720024050.56034123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 21:40:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 18.182%


Email Extensions
----------------
```

38. Pérdida detectada el día 19 de Julio a las 21:55:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720025550.55835123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 21:55:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 25.131%


Email Extensions
----------------
```

39. Pérdida detectada el día 19 de Julio a las 22:10:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720031050.54AC1123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 22:10:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 13.380%


Email Extensions
----------------
```

40. Pérdida detectada el día 19 de Julio a las 22:25:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720032550.56138123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 22:25:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 17.989%


Email Extensions
----------------
```

41. Pérdida detectada el día 19 de Julio a las 22:40:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720034050.52E98123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 22:40:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.423%


Email Extensions
----------------
```

42. Pérdida detectada el día 19 de Julio a las 22:55:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720035550.561F1123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 22:55:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.000%


Email Extensions
----------------
```

43. Pérdida detectada el día 19 de Julio a las 23:10:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720041050.54F06123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 23:10:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 13.492%


Email Extensions
----------------
```

44. Pérdida detectada el día 19 de Julio a las 23:25:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720042550.591DD123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 23:25:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 13.235%


Email Extensions
----------------
```

45. Pérdida detectada el día 19 de Julio a las 23:40:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720044050.61E7A123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 23:40:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.270%


Email Extensions
----------------
```

46. Pérdida detectada el día 19 de Julio a las 23:55:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720045550.52B18123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 23:55:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 22.222%


Email Extensions
----------------
```

47. Pérdida detectada el día 20 de Julio a las 00:10:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720051050.71241123740@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 00:10:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 13.281%


Email Extensions
----------------
```

48. Pérdida detectada el día 20 de Julio a las 00:25:50 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720052550.59711123740@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 00:25:50 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 15.862%


Email Extensions
----------------
```

49. Pérdida detectada el día 20 de Julio a las 00:39:52 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720053952.A7FD6123740@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 00:39:52 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.574%


Email Extensions
----------------
```

50. Pérdida detectada el día 20 de Julio a las 22:37:41 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721033741.0223B12372F@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 22:37:41 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 31.579%


Email Extensions
----------------
```

51. Pérdida detectada el día 20 de Julio a las 22:52:41 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721035241.09A4512372F@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 22:52:41 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 22.388%


Email Extensions
----------------
```

52. Pérdida detectada el día 20 de Julio a las 23:07:41 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721040741.19DD212372F@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 23:07:41 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 56.324%


Email Extensions
----------------
```

53. Pérdida detectada el día 20 de Julio a las 23:16:45 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721041645.802CF12372F@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 23:16:45 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 21.472%


Email Extensions
----------------
```

54. Pérdida detectada el día 20 de Julio a las 23:20:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721042049.37C0F121EAC@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 23:20:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 30.769%


Email Extensions
----------------
```

55. Pérdida detectada el día 20 de Julio a las 23:35:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721043549.44B3412372E@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 23:35:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 26.347%


Email Extensions
----------------
```

56. Pérdida detectada el día 20 de Julio a las 23:50:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721045049.36C9912372F@pp-HP-245-G4-PC>
Date: Thu, 20 Jul 2023 23:50:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 22.368%


Email Extensions
----------------
```

57. Pérdida detectada el día 21 de Julio a las 00:05:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721050549.30E9412372F@pp-HP-245-G4-PC>
Date: Fri, 21 Jul 2023 00:05:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 71.263%


Email Extensions
----------------
```

58. Pérdida detectada el día 21 de Julio a las 00:08:09 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230721050809.8885C12372F@pp-HP-245-G4-PC>
Date: Fri, 21 Jul 2023 00:08:09 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 25.000%


Email Extensions
----------------
```

59. Pérdida detectada el día 23 de Julio a las 23:43:05 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230724044305.154361237B1@pp-HP-245-G4-PC>
Date: Sun, 23 Jul 2023 23:43:05 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 36.810%


Email Extensions
----------------
```

60. Pérdida detectada el día 25 de Julio a las 22:08:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726030849.51CBA12002E@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 22:08:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.000%


Email Extensions
----------------
```

61. Pérdida detectada el día 25 de Julio a las 22:23:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726032349.94C5E12002F@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 22:23:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 71.963%


Email Extensions
----------------
```

62. Pérdida detectada el día 25 de Julio a las 22:38:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726033849.9773F120037@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 22:38:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 72.858%


Email Extensions
----------------
```

63. Pérdida detectada el día 25 de Julio a las 22:53:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726035349.8270B12002D@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 22:53:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 27.168%


Email Extensions
----------------
```

64. Pérdida detectada el día 25 de Julio a las 23:08:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726040849.8EDE2120035@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 23:08:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 36.495%


Email Extensions
----------------
```

65. Pérdida detectada el día 25 de Julio a las 23:23:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726042349.8BF88120035@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 23:23:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 23.567%


Email Extensions
----------------
```

66. Pérdida detectada el día 25 de Julio a las 23:38:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726043849.933C3120035@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 23:38:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 31.658%


Email Extensions
----------------
```

67. Pérdida detectada el día 25 de Julio a las 23:53:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726045349.8E896120035@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 23:53:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 65.743%


Email Extensions
---------------
```

68. Pérdida detectada el día 26 de Julio a las 00:08:49 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726050849.958A412004C@pp-HP-245-G4-PC>
Date: Wed, 26 Jul 2023 00:08:49 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 65.859%


Email Extensions
---------------
```

69. Pérdida detectada el día 26 de Julio a las 00:22:56 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726052256.1C30012004D@pp-HP-245-G4-PC>
Date: Wed, 26 Jul 2023 00:22:56 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 25.949%


Email Extensions
---------------
```

70. Pérdida detectada el día 28 de Julio a las 00:15:19 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230728051519.49C1B120097@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 00:15:19 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 25.613%

Email Extensions
---------------
```

71. Pérdida detectada el día 28 de Julio a las 00:30:19 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230728053019.41E5012009A@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 00:30:19 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 20.423%


Email Extensions
----------------
```

72. Pérdida detectada el día 28 de Julio a las 00:36:45 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230728235748.6BB2B12008C@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 00:36:45 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 15.000%


Email Extensions
----------------
```

73. Pérdida detectada el día 28 de Julio a las 22:04:43 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230729030443.960CE12009E@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 22:04:43 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 47.368%


Email Extensions
----------------
```

74. Pérdida detectada el día 28 de Julio a las 22:19:43 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230729031943.98C0712009E@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 22:19:43 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 39.676%


Email Extensions
----------------
```

75. Pérdida detectada el día 28 de Julio a las 22:34:43 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230729033443.A09DF12009E@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 22:34:43 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 13.068%


Email Extensions
----------------
```

76. Pérdida detectada el día 28 de Julio a las 22:49:43 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230729034943.A645512009E@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 22:49:43 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 17.262%


Email Extensions
----------------
```

77. Pérdida detectada el día 28 de Julio a las 22:50:45 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230729035045.436A912009E@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 22:50:45 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 23.077%


Email Extensions
----------------
```

78. Pérdida detectada el día 30 de Julio a las 16:56:23 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730215623.271C5120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 16:56:23 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 10.757%


Email Extensions
----------------
```

79. Pérdida detectada el día 31 de Julio a las 22:04:53 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230801030453.4B544120104@pp-HP-245-G4-PC>
Date: Mon, 31 Jul 2023 22:04:53 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 13.636%


Email Extensions
----------------
```

80. Pérdida detectada el día 31 de Julio a las 22:19:53 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Much_Loss
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230801031953.4E058120104@pp-HP-245-G4-PC>
Date: Mon, 31 Jul 2023 22:19:53 -0500 (-05)

Message: The capture loss script detected an estimated loss rate above 36.430%


Email Extensions
----------------
```

ANEXO G

Notificaciones de tipo CaptureLoss::Too_Little_Traffic

1. La primera notificación de este tipo es la que se muestra en la Figura 28.
2. Tráfico mínimo en la red el 18 de Julio a las 21:15:42 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Little_Traffic
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719021542.B6DCC12372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 21:15:42 -0500 (-05)

Message: Only observed 0 TCP ACKs and was expecting at least 1.


Email Extensions
----------------
```

3. Tráfico mínimo en la red el 18 de Julio a las 21:50:00 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Little_Traffic
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719025000.2B4AD123711@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 21:50:00 -0500 (-05)

Message: Only observed 0 TCP ACKs and was expecting at least 1.


Email Extensions
----------------
```

4. Tráfico mínimo en la red el 18 de Julio a las 22:05:00 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Little_Traffic
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719030500.1D806123711@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 22:05:00 -0500 (-05)

Message: Only observed 0 TCP ACKs and was expecting at least 1.


Email Extensions
----------------
```

5. Tráfico mínimo en la red el 18 de Julio a las 22:18:45 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Little_Traffic
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719031845.5C0701236F5@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 22:18:45 -0500 (-05)

Message: Only observed 0 TCP ACKs and was expecting at least 1.


Email Extensions
----------------
```

6. Tráfico mínimo en la red el 18 de Julio a las 23:54:07 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Little_Traffic
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230719045407.54B8912372D@pp-HP-245-G4-PC>
Date: Tue, 18 Jul 2023 23:54:07 -0500 (-05)

Message: Only observed 0 TCP ACKs and was expecting at least 1.


Email Extensions
----------------
```

7. Tráfico mínimo en la red el 23 de Julio a las 23:35:22 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] CaptureLoss::Too_Little_Traffic
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230724043522.160CF1237B1@pp-HP-245-G4-PC>
Date: Sun, 23 Jul 2023 23:35:22 -0500 (-05)

Message: Only observed 0 TCP ACKs and was expecting at least 1.


Email Extensions
----------------
```

ANEXO H

Notificaciones de tipo Traceroute::Detected

1. La primera notificación de este tipo es la que se muestra en la Figura 30.
2. Detección de un equipo realizando traceroutes el 19 de Julio a las 23:27:44 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] Traceroute::Detected
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230720042744.8911B123740@pp-HP-245-G4-PC>
Date: Wed, 19 Jul 2023 23:27:44 -0500 (-05)

Message: 2800:4b0:4434:93fd:8470:32d5:7bea:929a seems to be running traceroute using icmp

Address: 2800:4b0:4434:93fd:8470:32d5:7bea:929a

Email Extensions
----------------
orig/src hostname: <???>
```

ANEXO I

Notificaciones de tipo Scan::Port_Scan

1. La primera notificación de este tipo se muestra en la Figura 32.
2. Atacante cuya dirección IP es 192.168.43.84 escaneando varios puestos del equipo 192.168.43.47 en nuestra red el día 28 de Julio a las 23:02:51 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] Scan::Port_Scan
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230729040251.9069712009E@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 23:02:51 -0500 (-05)

Message: 192.168.43.84 scanned at least 15 unique ports of host 192.168.43.47 in 0m3s
Sub-message: local

Address: 192.168.43.84

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: pp-HP-245-G4-PC
```

3. Atacante cuya dirección IP es 192.168.43.84 escaneando varios puestos del equipo 192.168.43.47 en nuestra red el día 31 de Julio a las 22:28:06 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] Scan::Port_Scan
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230801032806.A1E2B120202@pp-HP-245-G4-PC>
Date: Mon, 31 Jul 2023 22:28:06 -0500 (-05)

Message: 192.168.43.84 scanned at least 15 unique ports of host 192.168.43.47 in 0m3s
Sub-message: local

Address: 192.168.43.84

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: pp-HP-245-G4-PC
```

4. Atacante cuya dirección IP es 192.168.43.84 escaneando varios puestos del equipo 192.168.43.47 en nuestra red el día 31 de Julio a las 23:29:16 horas.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] Scan::Port_Scan
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230801042916.DE069120202@pp-HP-245-G4-PC>
Date: Mon, 31 Jul 2023 23:29:16 -0500 (-05)

Message: 192.168.43.84 scanned at least 15 unique ports of host 192.168.43.47 in 0m22s
Sub-message: local

Address: 192.168.43.84

Email Extensions
----------------
resp/dst hostname: pp-HP-245-G4-PC

orig/src hostname: <???>
```

ANEXO J

Notificaciones de tipo SSL::Invalid_Server_Cert

1. La primera notificación de este tipo es la que se muestra en la Figura 33.
2. Validación del certificado fallido el día 25 de Julio a horas 23:07:36, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230726040736.118B2120035@pp-HP-245-G4-PC>
Date: Tue, 25 Jul 2023 23:07:36 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=*.prod.do.dsp.mp.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.72:57861 -> 20.54.24.169:443
Connection uid: Cj7bdl1T23TLZMoIWh

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

3. Validación del certificado fallido el día 28 de Julio a horas 00:00:48, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230728050048.896E812004B@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 00:00:48 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=*.prod.do.dsp.mp.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:63248 -> 51.104.162.168:443
Connection uid: CYBdqFJFC6gNXT3L6

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

4. Validación del certificado fallido el día 28 de Julio a horas 22:05:16, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230729030516.0FE3612009E@pp-HP-245-G4-PC>
Date: Fri, 28 Jul 2023 22:05:16 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:49786 -> 51.104.15.253:443
Connection uid: CHtC223YrMW5vPOO59

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

5. Validación del certificado fallido el día 30 de Julio a horas 17:27:13, proveniente del Cloud Service de Huawei.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730222713.CB700120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 17:27:13 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=grs.dbankcloud.com,OU=Huawei CBG Cloud Service,O=Huawei,C=CN

Connection: 192.168.43.84:50130 -> 94.74.81.23:443
Connection uid: Cll1WK26JMz3Ouvqs8

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: ecs-94-74-81-23.compute.hwclouds-dns.com
```

6. Validación del certificado fallido el día 30 de Julio a horas 17:27:14, proveniente del Cloud Service de Huawei.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730222714.C2D9F120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 17:27:14 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=grs.dbankcloud.com,OU=Huawei CBG Cloud Service,O=Huawei,C=CN

Connection: 192.168.43.84:50135 -> 94.74.81.37:443
Connection uid: CxbJcd1FaR9lTRnhIa

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: ecs-94-74-81-37.compute.hwclouds-dns.com
```

7. Validación del certificado fallido el día 30 de Julio a horas 18:32:37, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730233237.5EBC3120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 18:32:37 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=wdcp.microsoft.com,OU=Microsoft Corporation,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US

Connection: 192.168.43.84:50485 -> 20.201.21.178:443
Connection uid: CtJI0flchSiX5rRPd

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

8. Validación del certificado fallido el día 30 de Julio a horas 18:57:24, proveniente del servicio de actualización de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730235725.07D6C120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 18:57:24 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=slscr.update.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:50590 -> 52.165.165.26:443
Connection uid: CJszI57IqcYv6kdfb

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

9. Validación del certificado fallido el día 30 de Julio a horas 18:57:26, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730235726.628EE120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 18:57:26 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:50591 -> 52.182.143.211:443
Connection uid: CiDii21j4ja54X3kvc

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

10. Validación del certificado fallido el día 30 de Julio a horas 18:57:27, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730235727.D9DCF120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 18:57:27 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:50593 -> 51.104.15.252:443
Connection uid: C80VdP26g0L49vm1Qh

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

11. Validación del certificado fallido el día 30 de Julio a horas 18:57:32, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230730235732.DE6D9120105@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 18:57:32 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:50596 -> 52.178.17.3:443
Connection uid: C72Wrz4sx5jpW0XBr6

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

12. Validación del certificado fallido el día 30 de Julio a horas 21:32:07, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230731023207.B6ECE120093@pp-HP-245-G4-PC>
Date: Sun, 30 Jul 2023 21:32:07 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:57352 -> 20.189.173.10:443
Connection uid: CiYoOZj1GBefViirg

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

13. Validación del certificado fallido el día 31 de Julio a horas 22:23:04, proveniente de algún producto o servicio de Microsoft.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230801032304.DB1BE120104@pp-HP-245-G4-PC>
Date: Mon, 31 Jul 2023 22:23:04 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=api.cdp.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US

Connection: 192.168.43.84:60002 -> 13.67.191.143:443
Connection uid: CmbVP619XnpSj0Irak

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: <???>
```

14. Validación del certificado fallido el día 31 de Julio a horas 22:58:33, proveniente del Cloud Service de Huawei.

```
From: Zeek <zeek@pp-HP-245-G4-PC>
Subject: [Zeek] SSL::Invalid_Server_Cert
To: root@localhost
User-Agent: Zeek/5.0.9
Message-Id: <20230801035833.5B1B6120202@pp-HP-245-G4-PC>
Date: Mon, 31 Jul 2023 22:58:33 -0500 (-05)

Message: SSL certificate validation failed with (unable to get local issuer certificate)
Sub-message: CN=grs.dbankcloud.com,OU=Huawei CBG Cloud Service,O=Huawei,C=CN

Connection: 192.168.43.84:50100 -> 94.74.81.37:443
Connection uid: C3ZKvS2mFeTK6dWaj8

Email Extensions
----------------
orig/src hostname: <???>

resp/dst hostname: ecs-94-74-81-37.compute.hwclouds-dns.com
```

UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGIA Y CIVIL ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

CONSTANCIA DE PRIMERA MATRICULA Nº 040-2023-FIMGC-EPIS-UNSCH/EFGM

La Dirección de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería de Minas, Geología y Civil, de la Universidad Nacional de San Cristóbal de Huamanga, deja constancia que el señor **AMORHIN ROJAS HUARHUACHI;** con DNI N° **70812214** y código universitario N° **27120620**, estudiante de la Escuela Profesional de Ingeniería de Sistemas, inició sus estudios en el semestre académico **2012-I** de fecha **11 de marzo del 2013**.

Se expide la presente constancia a solicitud de la interesada para fines que estime conveniente.

Ayacucho, 24 de octubre del 2023.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA
FACULTAD DE ING. MINAS, GEOLOGIA Y CIVIL
M. Sc. Ing. J. Ernesto Estrada Cárdenas
DECANO

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
Mg. Edith [illegible] Mollote
DIRECTORA

C.c.
Archivo
EFGM/wdvp

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
Av. Independencia S/N
Ciudad Universitaria
Tel. 066 - 327273

UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

N° 043-2023

CONSTANCIA DE EGRESADO

La Dirección de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería de Minas, Geología y Civil, de la Universidad Nacional de San Cristóbal de Huamanga (UNSCH), deja constancia que el señor **Amorhin ROJAS HUARHUACHI**, con DNI N° **70812214** y código universitario N° **27120620**, estudiante de la Escuela Profesional de Ingeniería de Sistemas, culminó sus estudios con el **Plan 2005-R**, en el semestre académico **2020-I** de fecha **07 de enero del 2020.**

Se expide la presente constancia a solicitud del interesado para fines estrictamente académicos.

Ayacucho, 24 de octubre del 2023.

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA
FACULTAD DE ING. MINAS, GEOLOGIA Y CIVIL
M. Sc. Ing. J. Ernesto Estrada Cárdenas
DECANO

UNIVERSIDAD NACIONAL DE SAN CRISTOBAL DE HUAMANGA
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS
Mg. Edith F. Quevara Morote
DIRECTORA

C.c.
Arch.
EFGM/wdvp

ESCUELA PROFESIONAL DE
INGENIERIA DE SISTEMAS
Av. Independencia S/N
Ciudad Universitaria
Tel. 066 - 327273

CONSTANCIA DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

CONSTANCIA N° 061-2023-FIMGC

El que suscribe; responsable verificador de originalidad de trabajos de tesis de pregrado con el software Turnitin, en segunda instancia para las **Escuelas Profesionales** de la **Facultad de Ingeniería de Minas, Geología y Civil**; en cumplimiento a la **Resolución de Consejo Universitario N° 039-2021-UNSCH-CU**, Reglamento de Originalidad de Trabajos de Investigación de la Universidad Nacional San Cristóbal de Huamanga y **Resolución Decanal N° 288-2023-FIMGC- UNSCH-D**, deja constancia de originalidad de trabajo de investigación, que el/la Sr./Srta.

Apellidos y Nombres	:	ROJAS HUARHUACHI, Amorhin
Escuela Profesional	:	INGENIERÍA SISTEMAS
Título de la Tesis	:	"MONITOR DE SEGURIDAD DE RED ZEEK OPEN SOURCE COMO MECANISMO DE SEGURIDAD EMPRESARIAL EN ENTORNOS LIBRES, 2023"
Evaluación de la Originalidad	:	13 % Índice de Similitud
Identificador de la entrega	:	2149625934

Por tanto, según los Artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación, es **PROCEDENTE** otorgar la **Constancia de Originalidad** para los fines que crea conveniente.

En señal de conformidad y verificación se firma la presente constancia

Ayacucho, 22 de agosto del 2023

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
Facultad de Ingeniería de Minas, Geología y Civil

Mg. Ing. Christian LEZAMA CUELLAR
Verificador de Originalidad de Trabajos de Tesis de Pregrado
Departamento Académicos de Matemática y Física

Con depósito para Sustentación y Tramites
Cc. Archivo

“MONITOR DE SEGURIDAD DE RED ZEEK OPEN SOURCE COMO MECANISMO DE SEGURIDAD EMPRESARIAL EN ENTORNOS LIBRES, 2023”

por Amorhin Rojas Huarhuachi

Fecha de entrega: 22-ago-2023 04:50p.m. (UTC-0500)
Identificador de la entrega: 2149625934
Nombre del archivo: Tesis_Amorhin_Rojas_Huarhuachi_EPIS.pdf (5.68M)
Total de palabras: 19471
Total de caracteres: 112268

“MONITOR DE SEGURIDAD DE RED ZEEK OPEN SOURCE COMO MECANISMO DE SEGURIDAD EMPRESARIAL EN ENTORNOS LIBRES, 2023”

INFORME DE ORIGINALIDAD

13%	9%	1%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	mirrors.xmission.com Fuente de Internet	8%
2	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	4%
3	Luiza Romani Ferreira Banov. "Grafias da dança em deslocamento: experiência, memória e transmissibilidade", Universidade de Sao Paulo, Agencia USP de Gestao da Informacao Academica (AGUIA), 2020 Publicación	1%
4	"Tendencias en la Investigación Universitaria. Una visión desde Latinoamérica", Alianza de Investigadores Internacionales SAS, 2020 Publicación	<1%
5	ports.macports.org Fuente de Internet	<1%

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		

ACTA DE SUSTENTACIÓN DE TESIS

ACTA N° 071-2023-FIMGC

En la ciudad de Ayacucho, en cumplimiento a la **RESOLUCIÓN DECANAL N° 349-2023-FIMGC-D**, siendo los seis días del mes de setiembre del 2023, a horas 5:00 pm.; se reunieron los jurados del acto de sustentación, en el Auditórium virtual google meet del Campus Universitario de la Universidad Nacional de San Cristóbal de Huamanga.

Siendo el Jurado de la sustentación de tesis compuesto por el presidente el **Dr. Ing. Efraín Elías PORRAS FLORES,** Jurado el **MSc. Ing. Edem Jersson TERRAZA HUAMÁN,** Jurado el **MSc. Ing. Javier PORTILLO QUISPE,** Jurado - Asesor el **Dr. Ing. Hubner JANAMPA PATILLA** y secretario del proceso el **Mg. Ing. Christian LEZAMA CUELLAR,** con el objetivo de recepcionar la sustentación de la tesis denominada titulado: **"MONITOR DE SEGURIDAD DE RED ZEEK OPEN SOURCE COMO MECANISMO DE SEGURIDAD EMPRESARIAL EN ENTORNOS LIBRES, 2023,** presentado por el/la Sr./Srta., **AMORHIN ROJAS HUARHUACHI,** Bachiller en **Ingeniería de Sistemas.**

El Jurado luego de haber recepcionado la sustentación de la tesis y realizado las preguntas, el sustentante al haber dado respuesta a las preguntas, y el Jurado haber deliberado; califica con la nota aprobatoria de **14 (catorce).**

En fe de lo cual, se firma la presente acta, por los miembros integrantes del proceso de sustentación.

UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA
FACULTAD DE INGENIERÍA DE MINAS GEOLOGÍA Y CIVIL
Dr. Efraín Elías Porras Flores
DECANO

Firmado digitalmente por Dr.Ing. Efrain Elias Porras Flores
Fecha: 2023.09.08 19:16:38 -05'00'

Dr. Ing. Efraín Elías PORRAS FLORES
Presidente

MSc. Ing. Edem Jersson TERRAZA HUAMÁN
Jurado

Dr. Ing. Hubner JANAMPA PATILLA
Jurado Asesor

MSc. Ing. Javier PORTILLO QUISPE
Jurado

Mg. Ing. Christian LEZAMA CUELLAR
Secretario del Proceso
Departamento Académico de Matemática y Física

C.c.:
Bach. AMORHIN ROJAS HUARHUACHI
Jurados (4)
Archivo