UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN
MAYO 2024 - AGOSTO 2025

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

SEGURIDAD EN REDES DE DATOS CON LA AYUDA DEL IDS SNORT EN KALI LINUX EN EL DATACENTER DEL CUERPO DE BOMBEROS DE BABAHOYO

ESTUDIANTE:
EVELYN JULISSA PAREDES JURADO

TUTOR:
ING. RAUL RAMOS

AÑO 2024

SEGURIDAD EN REDES DE DATOS CON LA AYUDA DEL IDS SNORT EN KALI LINUX EN EL DATACENTER DEL CUERPO DE BOMBEROS DE BABAHOYO

SECURITY IN DATA NETWORKS WITH THE HELP OF IDS SNORT IN KALI LINUX IN THE DATA CENTER OF THE BABAHOYO FIRE DEPARTMENT.

RESUMEN

El estudio de caso titulado "Seguridad en Redes de Datos con la Ayuda del IDS Snort en Kali Linux en el datacenter del Cuerpo de Bomberos de Babahoyo" se centra en la implementación y análisis de un Sistema de Detección de Intrusos (IDS) utilizando Snort para mejorar la seguridad de la red en el Cuerpo de Bomberos de Babahoyo. La investigación aborda la creciente amenaza cibernética que enfrenta esta entidad, destacando la insuficiencia de los métodos tradicionales de seguridad, como firewalls y antivirus, para enfrentar ataques sofisticados.

El documento describe cómo Snort, en conjunto con la plataforma Kali Linux, permite detectar, en tiempo real, posibles intrusiones y amenazas a la red, mejorando así la respuesta del personal de seguridad ante incidentes cibernéticos. La implementación de Snort resultó en una mejora significativa en la detección de amenazas y la reducción de falsos positivos y negativos, lo que aumentó la eficiencia operativa y la protección de la infraestructura tecnológica.

Palabras clave: Seguridad en redes, IDS (Sistema de Detección de Intrusos), Snort, Kali Linux, ciberseguridad, protección de datos, ataques cibernéticos, falsos positivos/negativos, respuesta ante incidentes, datacenter.

ABSTRACT

The case study entitled “Data Network Security with the Help of Snort IDS on Kali Linux in the Babahoyo Fire Department Datacenter” focuses on the implementation and analysis of an Intrusion Detection System (IDS) using Snort to improve network security at the Babahoyo Fire Department. The research addresses the growing cyber threat faced by this entity, highlighting the inadequacy of traditional security methods, such as firewalls and antivirus, to deal with sophisticated attacks.

The paper describes how Snort, in conjunction with the Kali Linux platform, enables real-time detection of potential intrusions and threats to the network, thus improving the response of security personnel to cyber incidents. The implementation of Snort resulted in a significant improvement in threat detection and the reduction of false positives and negatives, which increased operational efficiency and protection of the technological infrastructure.

Keywords: Network security, IDS (Intrusion Detection System), Snort, Kali Linux, cybersecurity, data protection, cyber-attacks, false positives/negatives, incident response, datacenter.

ÍNDICE

PLANTEAMIENTO DEL PROBLEMA

En las organizaciones de todo el mundo deben proteger sus sistemas y redes informáticas de las crecientes amenazas cibernéticas. Confiar cada vez más en la tecnología y la conexión a internet han dejado a estas entidades vulnerables a una variedad de riesgos, desde ataques de malware y ransomware hasta intentos de acceso no autorizado y robo de datos confidenciales.

El Cuerpo de Bombero de Babahoyo es una unidad especializada para la seguridad y bienestar de la comunidad, pero que también presenta estos ataques cibernéticos. La infraestructura tecnológica que tiene está compuesta por un centro de datos con redes tanto cableadas como inalámbricas, la cual es muy importante para poder manejar de la información y la relación de sus actividades. Pero, ha recibido diversos ataques esta infraestructura, especialmente en la noche.

A continuación, se describe dos de los ataques más comunes que presenta el Cuerpo de Bomberos de Babahoyo:

- Ataques de Inyección: El objetivo de estos ataques es explotar las diversas vulnerabilidades existentes en la base de datos, para extraer o manipular diversa información inyectan códigos maliciosos.

- Ataques de Saturación (Denegación de Servicio - DoS): A diferencia del anterior estos ataques buscan colapsar los servidores de la red, logrando la caída de servicios esenciales y la detención de las operaciones del cuerpo de bomberos.

De los principales problemas que aflige al personal de seguridad informática del Cuerpo de Bomberos es la detección exacta y efectiva de ataques en su entorno informático. Los

enfoques comunes de seguridad, como firewalls y antivirus, han demostrado ser insuficientes para hacer frente a las técnicas de ataque cada vez más sofisticadas. Los atacantes han desarrollado métodos refinados para evadir estos controles, obligando a la institución a buscar soluciones más robustas y adaptables.

La creciente complejidad de las redes del Cuerpo de Bomberos, caracterizada por la combinación de redes inalámbricas y cableadas sin una adecuada segmentación y protección, y la falta de un sistema de monitoreo continuo, ha ampliado significativamente la superficie de ataque. Estas circunstancias proyectan nuevos retos para detección de intrusos, porque los encargados de la seguridad deben combatir con un ambiente que es cada día más vulnerable y dinámico.

Complementario a esto, estos tipos de ataques cibernéticos van avanzando, con técnicas como la ingeniería social, al igual que la obtención de vulnerabilidades conocidas y el uso de herramientas automatizadas. Estas amenazas avanzadas han son capaces de evadir los controles de seguridad usados tradicionalmente, lo que ha obligado a la institución a modificar sus estrategias de protección.

Uno de los casos que ejemplifica esta problemática es un ataque nocturno al datacenter del Cuerpo de Bomberos, donde los atacantes lograron infiltrarse en la red y causar la caída de servicios críticos mediante un ataque de saturación. Esto formó un gran impacto significativo en la efectividad del Cuerpo de Bomberos, la cual puso en riesgo la veracidad de las respuestas ante las emergencias, lo que afectaba la confianza de la comunidad.

La investigación que se dio luego hizo conocer que algunos sistemas de seguridad tradicionales del datacenter, como firewalls y software antivirus, no eran lo suficiente

para poder detener los ataques. Aquellos atacantes se benefician de las vulnerabilidades más comunes para evitar estos tipos los controles y así no ser detectados.

Dicho evento hizo que de manera urgente haya la necesidad de aplicar soluciones más eficientes y efectivas dentro del Cuerpo de bomberos. El personal encargado del área de seguridad en redes debe estar preparados con tecnologías y herramientas la cual permitan tener una respuesta rápida de los incidentes que se presentan, para evitar que algún ataque tenga éxito.

La complejidad de red crece y llegan nuevas tecnologías que amplían la superficie del ataque, la cual la detección de intrusiones genera cada vez más desafíos. Los expertos en seguridad tienen que conocer estas nuevas tendencias para elaborar estrategias y ajustarlas en consecuencia.

Dadas las circunstancias, se debe desarrollar efectivas soluciones, mediante la exploración, que permitan que el Cuerpo de Bomberos, específicamente el equipo de sistemas, para que puedan responder e identificar los incidentes de seguridad que puedan presentarse. La prueba de la herramienta y diversas reglas de Snort para la detección de intrusos, se convierte en una de las prioridades para poder detectar con mayor rapidez los ataques para tomar las medidas necesarias y proteger los datos importantes dentro de la entidad logrando una mejor continuidad y seguridad de la organización.

JUSTIFICACIÓN

En estudio es significativo porque aborda un tema real y urgente de la seguridad de la red de datos del Departamento de Bomberos de Babahoyo. Proteger la información de los trabajadores sobre todo el cuidado de la infraestructura tecnológica es fundamental porque los atacantes pueden aprovechar cualquier vulnerabilidad de seguridad para afectar la integridad, la disponibilidad, la confidencialidad de los datos y servicios principales que administran. Cada vez que las amenazas se vuelven más difíciles, más importante es implementar soluciones que estén más allá de los tradicionales enfoques de seguridad.

La implementación de un sistema de detección de intrusos (IDS) como Snort tiene como propósito mejorar significativamente a la seguridad de la infraestructura tecnológica del Cuerpo de Bomberos de Babahoyo. Este sistema gracias a sus funciones avanzadas tiene la capacidad de detectar los incidentes en tiempo real. Esto nos ayuda a identificar maneras más efectivas para contraatacar las posibles intrusiones, y que el personal pueda reaccionar con más rapidez.

Adicional a mejorar la seguridad dentro del establecimiento, esta investigación ayuda a poder tener más información sobre técnicas y reglas que ayudarán a otros establecimientos a que también puedan tener una mejor detección de intrusos, y así estén preparados para mitigar los riesgos de ingreso a la información confidencial.

Al igual que en los resultados de otros casos como lo es en la Universidad de Purdue la aplicación de Snort ayudó a poder mitigar varios intentos de ataques entre ellos de malware que pudo haber comprometido datos sensibles si no se notificaban a tiempo,

también hubo reducción de incidentes gracias a la alerta que la herramienta Snort daba en tiempo real.

Como resultado, la seguridad cibernética se convierte en un elemento integral de la adaptabilidad y eficiencia operativa del Departamento de Bomberos de Babahoyo, lo que garantiza que la agencia pueda responder adecuadamente a las emergencias sin verse comprometida ni afectar su capacidad de operar.

OBJETIVOS

- **Objetivo general:**

Analizar la implementación de un Sistema de Detección de Intrusos (IDS) utilizando Snort en Kali Linux para la mejora de la seguridad de la red de datos del Cuerpo de Bomberos de Babahoyo.

- **Objetivos específicos:**

1. Recolectar información necesaria de los conceptos importantes que aporte a la investigación para la seguridad de redes en el Cuerpo de Bomberos de Babahoyo.
2. Realizar la configuración de las reglas personalizadas en Snort para los ataques concurrentes en el entorno presente.
3. Evaluar la efectividad de Snort mediante pruebas controladas y simulaciones de ataques en la red del Cuerpo de Bomberos de Babahoyo.

LÍNEAS DE INVESTIGACIÓN

Línea de investigación: Sistemas de información y comunicación, emprendimiento e innovación.

La línea de investigación se relaciona al estudio de caso porque los sistemas de información tienen relación con los IDS la cual es fundamental para detectar amenazas de seguridad en las redes informáticas y la integración de estas herramientas, puede ser considerado una forma de emprender o innovar dentro del campo de la ciberseguridad.

Sublínea de investigación: Redes y tecnologías inteligentes de software y hardware.

La sublínea se relaciona con la investigación porque este tema tiene una profunda relación son las redes, ya que por medio de ellas es que se producen los diferentes ataques, además el IDS que se está utilizando tiene que ver mucho los protocolos de la comunicación y vulnerabilidades que pueden ser explotadas. Además, se requiere la integración de Snort con otras herramientas de seguridad requiere el estudio y la implementación de tecnologías inteligentes de software y hardware para mejorar la detección, la respuesta y la gestión de incidentes de seguridad en la red.

MARCO CONCEPTUAL

1. **Seguridad en Redes de Datos**:

Cualquier actividad, política, procesos o tecnologías que este hecha para proteger los activos digitales de una organización o individuo de las amenazas es considerado ciberseguridad. Su principal función es impedir que aquellos atacantes puedan acceder a información confidencial mediante la red interna de las computadoras u otros dispositivos protegiendo así los datos, sistemas y dispositivos en los que están almacenados (Santos Chavez, 2024).

Amenazas actuales a la seguridad de las redes:

Denegación de servicio (DDoS):

Los ataques distribuidos de denegación de servicio (DDoS) explotan los límites de capacidad de los recursos de la red, como la infraestructura del sitio web, enviando muchas solicitudes para saturar su energía y estropearlos (Kaspersky, 2021).

Malware:

El malware es un software diseñado para infectar, dañar o acceder a sistemas informáticos, comprometiendo su seguridad y privacidad. Puede robar datos financieros y confidenciales para cometer fraudes y otros delitos que afectan a PC con Windows, Mac y dispositivos móviles (Belcic, Avast, 2023)

Intrusiones:

Los ataques de intrusión de malware son eventos en los que un atacante utiliza malware para obtener acceso no autorizado a un sistema o red. Este software malicioso, conocido como malware, incluye varios tipos, como virus, gusanos, troyanos, ransomware y

spyware. Estos ataques suelen iniciarse cuando un usuario inicia o descarga accidentalmente un archivo infectado o visita un sitio web comprometido que explota vulnerabilidades en el software o el sistema operativo (Cilleruelo, 2024).

Vulnerabilidades de red:

Es algún error del sistema informático que es utilizado por los atacantes para violar la seguridad de la información, es decir su integridad, disponibilidad y confidencialidad (Micucci, 2024).

Inyección de códigos SQL:

Estos tipos de ataques solo se permiten cuando una página web no tiene una entrada adecuada , la cual el atacante introduce códigos SQL maliciosos convirtiéndose en un tipo de malware conocido como una carga útil, lo que quiere decir que por medio de esas entradas el atacante manda códigos SQL haciéndose pasa como una consulta legal. (Belcic, Avast, 2020)

Probabilidad de vulnerabilidades según el tipo de amenazas:

Área del Sistema	Tipo de vulnerabilidad	Porcentaje
Red	Denegación de servicio (DDoS)	25%
Dispositivos	Malware	20%
Seguridad de RED	Intrusiones	15%

Infraestructura	Vulnerabilidades de red	20%
Aplicaciones web	Inyección de código SQL	20%

Métodos y tecnologías para asegurar redes:

Firewalls:

Es un componente de la computadora la cual ayuda a controlar el tráfico que sale y el que entra de la red o dispositivo para poder bloquear los datos que no están cumpliendo ciertos estándares de seguridad. Es como una barrera entre la red local y una red pública. Estos examinan los datos que quieren ingresar al igual que los que salen de la red interna, y solo pasan los que cumplen aquellos criterios y bloquea a los que no lo hacen (Gómez, delta, 2024).

Sistemas de detección de intrusiones (IDS):

Los IDS están en constante monitoreo de las redes y de aquellos dispositivos que están conectados a estos sistemas, pero no puede realizar acciones a los atacantes, solo generan una alarma cuando se presenta algún tipo de intrusiones que el sistema haya detectado. Estos sistemas lo que hacen es solo analizar cada comportamiento y determinan si hay algún movimiento inusual para notificar a los administradores o el personal de la organización y estos tomen las medidas pertinentes para dicho caso. Para que esto sea eficaz el IDS necesita ser auto escaneado sin que esto sobrecargue los recursos de los mismos. La ventaja de estos sistemas es que son compatibles con todos los sistemas

operativos existentes, además están preparados para que puedan funcionar aún si el S.O falla (Escalante, Abcxperts, 2023).

Vamos a emplear uno de los muchos sistemas que actualmente existen para poder monitorear y analizar el tráfico de red en busca de posibles amenazas o actividad maliciosa.

- Snort:

Snort se basa en libpcap, una herramienta comúnmente utilizada en rastreadores de tráfico TCP/IP y rastreadores de paquetes. Al analizar protocolos, buscar y comparar contenido, Snort puede detectar varios métodos de ataque, como denegación de servicio, desbordamiento de búfer, ataques CGI, escaneo de puertos encubiertos y sondas SMB. Cuando se detecta un comportamiento sospechoso, Snort envía alertas en tiempo real al registro del sistema, a un archivo de alerta separado o a una ventana emergente (Atico, 2021).

- Kali Linux:

Es un sistema que parte de Linux que está diseñada específicamente para tareas relacionadas en el ámbito de la seguridad la cuales, entra el análisis de redes, ataques inalámbricos e investigaciones. Es usado por la mayoría de usuario estos profesionales hasta estudiantes debido a la variedad de pruebas que pueden hacen sobre seguridad y también a la gran cantidad de herramientas que facilitan esta operación lo que convierte a Kali Linux en una de las distribuciones de seguridad más populares y efectivas (Altube, 2023).

Sistemas de prevención de intrusiones (IPS):

Los IPS están diseñados para poder detener las amenazas en tiempo real, actualmente existen muchos tipos de ataques la cuales estos sistemas son los que ayudan a poder prevenirlos, lo hacen a través de una evaluación de validez de los paquetes de datos, con la referencia de base de datos que poseen donde analizan los comportamientos maliciosos, incluso de firmas de amenazas (Escalante, Abc Xperts, 2023).

Redes Privadas Virtuales (VPN):

Un VPN es aquel servicio que tiene una conexión en línea de manera segura y cifrada, lo que permite el incremento de la privacidad a los usuarios y evita los bloqueos geográficos. La red privada virtual permite envío y recepción segura de los datos. Estas se usan en redes que no están tan seguras para poder protegerse de las vigilancias de las ISP o puntos de acceso de Wi-Fi que no estén seguras, haciendo que se oculte los historiales, las direcciones IP y cualquier otra actividad web incluyendo la ubicación (Gillis, 2021).

Antivirus ESET:

ESET ofrece una solución antivirus para servidores que protege contra diversas amenazas de malware, asegurando un funcionamiento seguro y eficiente mediante análisis en tiempo real y detección proactiva (Serra, 2023).

Tecnologías para asegurar redes	**Descripción**	**Ventajas**	**Desventajas**	**Costo**

Firewalls	Firewall de red	Controla el tráfico de red, reglas personalizables	No detecta malware y requiere de conocimientos técnicos	Gratuito
Snort	Sistema de detección de intrusos	Detecta ataques en tiempo real, alta detección de malware	Requiere conocimientos técnicos	Gratuito
Kali Linux	Distribución para pruebas de seguridad	Incluye herramientas de prueba de penetración, análisis de redes	Requiere conocimientos técnicos , puede ser complejos.	Gratuito
Redes Privadas Virtuales (VPN)	Red Privada Virtual	Encripta tráfico de red, protege datos, acceso remoto seguro	Puede ser lento y requiere de configuración	De pago/gratuito
Antivirus ESET	Software antivirus	Detecta y elimina malware,	No detecta ataques de red, puede ser lento	Pago

		protección en tiempo real.		

Datacenter del Cuerpo de Bomberos de Babahoyo:

Dentro de la infraestructura de red encontramos que tiene conexiones de tipo bus que integra 2 switches la cual tiene 24 puertos Gigabyte cada uno y un servidor central.

Tienen redes inalámbricas y cableadas, utilizan un protocolo TCP-IP , La red en la que opera es de IPV4, pero la que reciben del proveedor es de IPV6.

La red inalámbrica es una red en malla o también conocida como mesh que permite que todos los dispositivos dentro de la entidad permanezcan conectados entre sí para evitar interferencias y garantizar la continuidad del servicio. Esta red utiliza Wi-Fi 5 con canales de 2,4 GHz y 5,8 GHz, los dispositivos son de la marca Huawei, modelo Wi-Fi AX2. La infraestructura incluye un cableado estructurado con respaldo de batería UPS, lo que garantiza un funcionamiento continuo en caso de un corte de energía. La base de datos de información del usuario se almacena en el servidor local al igual que en el proveedor de hosting y la red del dominio son administrados por Ecua Hosting.

En términos de seguridad, la red cuenta con un firewall que implementa reglas básicas para bloquear malware, y un antivirus de servidor de ESET. También se emplea seguridad de clave pictográfica para aleatorizar y proteger los datos mediante encriptación WPA. La red es utilizada principalmente para la revisión de datos y opera con bases de datos MySQL.

El Cuerpo de Bomberos de Babahoyo tiene 15 áreas diferentes que se conectan y distribuyen a través de los dos switches existentes, asegurando una conectividad eficiente y segura para todas sus operaciones.

Tecnologías Emergentes en Seguridad de Redes:

a. Redes 5G

El despliegue generalizado de redes 5G aumenta la superficie de ataque, incluyendo más dispositivos y mayores cantidades de datos. Además, la fragmentación y virtualización de la red 5G crean nuevas vulnerabilidades de seguridad que requieren una segmentación y un aislamiento efectivos para evitar el acceso no autorizado y la fuga de datos (Flores, 2022)

Cumplimiento Normativo y Mejores Prácticas:

ISO 27001:

Las normas ISO 27001 se enfoca en es SGSI la cual requiere tiene requisitos que ayudan a mejorar continuamente, implementando y manteniendo la seguridad de la información. Es la norma la cual en las organizaciones pueden identificar y organizar los diferentes riesgos en la seguridad de la información (Global Suite Solutions, 2023).

Configuración y Gestión de Redes en datacenters:

Las VLAN, o «Virtual LAN», permiten crear redes lógicas independientes dentro de una red física utilizando switches gestionables que soportan VLANs para segmentar adecuadamente la red. Es esencial que los enrutadores también sean compatibles con VLAN para gestionar la comunicación entre ellas. En la actualidad, la mayoría de los

routers profesionales y sistemas operativos diseñados para firewalls/routers, como pfSense u OPNsense, son compatibles con VLAN, ya que se ha convertido en un estándar (Asenjo, 2024).

Protocolos de Red y Comunicación:

Según (Limones, 2021),La gestión de la configuración de la red implica organizar y mantener información sobre todos los componentes de una red informática. Cuando es necesario reparar, modificar, ampliar o modernizar las redes, los administradores utilizan bases de datos de gestión de configuración para determinar el mejor enfoque. Esta base de datos contiene la ubicación, dirección IP o dirección de red de todos los dispositivos de hardware, así como información sobre la configuración predeterminada, programas, versiones y actualizaciones instaladas en la computadora en línea.

TCP/IP

TCP/IP, o Protocolo de control de transmisión/Protocolo de Internet, es un conjunto estándar de reglas que admiten la comunicación entre computadoras en redes como Internet. Aunque una computadora puede realizar ciertas tareas por sí sola, sus capacidades mejoran enormemente cuando puede trabajar con otros dispositivos. Muchas de nuestras acciones, como enviar un correo electrónico, ver Netflix u obtener direcciones, dependen de esta relación. Estas computadoras pueden ser de diferentes marcas y estar ubicadas en diferentes partes del mundo, y los usuarios y programas que las controlan pueden hablar diferentes idiomas, tanto humanos como informáticos (Fisher, 2019).

Metodologías de pruebas de penetración y simulación de ataques:

b. Prueba de penetración

- Pentesting o prueba de penetración es el proceso de evaluar la seguridad de un sistema informático, red o aplicación mediante la simulación de ataques de piratas informáticos éticos para identificar vulnerabilidades de seguridad. Aquellos que están especializados en combatir en esta área se enfocan en puntos de no autorizados tanto de entrada como traseras, o incluso de incorrectas configuraciones y vulnerabilidades, usando las técnicas y herramientas avanzadas para poder tener un análisis de todos los puntos. Con el objetivo de poder conocerlas, para que las organizaciones o entidades puedan tomar las medidas necesarias antes de que los atacantes se den cuenta. En última instancia, las pruebas de penetración fortalecen la seguridad de una empresa y protegen sus activos digitales y datos confidenciales (Chavarría, 2023).

Análisis de tráfico de red y patrones de comportamiento:

Los ciberataques en los últimos años han crecido en gran manera, uno de los grandes es en que en España ha aumentado un 43% en el año 2023 según el informe de Hiscox realizado en el 2023 (Dominguez, 2023).

MARCO METODOLÓGICO

Este estudio de caso adoptará un enfoque cualitativo, ya que se centra en la comprensión y análisis en profundidad del uso del sistema de detección de intrusos (IDS) Snort en el entorno informático del Cuerpo de Bomberos de Babahoyo. Asimismo, se caracterizará por ser de tipo descriptivo, ya que se busca detallar las características, funcionalidades y capacidades de Snort en la detección y análisis de intrusos en la red de dicha institución.

El diseño de la investigación será un estudio de caso único, enfocado en el análisis exhaustivo de la implementación y uso de Snort en el área de sistemas del Cuerpo de Bomberos de Babahoyo. Para este estudio de caso, la población estará conformada por el personal del área de sistemas del Cuerpo de Bomberos de Babahoyo, entre ellos están el jefe de las TICs, el proveedor de la red, encargado de la administración y supervisión de la red informática de la institución. Debido al tamaño reducido del equipo de sistemas, se trabajará con la totalidad de la población sin necesidad de definir una muestra.

Las principales técnicas e instrumentos de recolección de datos que se emplearán en este estudio de caso son: entrevistas semiestructuradas al personal del área de sistemas, observación directa del funcionamiento y desempeño de Snort en el entorno informático del Cuerpo de Bomberos, y análisis relacionado con la infraestructura tecnológica y las políticas de seguridad de la institución.

Con los datos recolectados se realizará un análisis donde se documente los detalles relevantes que ayuden a comprender mejor el contexto de la organización con respecto al tema investigado enfocado a la seguridad.

Finalmente, cabe recalcar que se respetarán los principios éticos en la realización de este estudio.

RESULTADOS

Los resultados de este caso tienen una fijación profunda sobre la comprensión sobre el uso IDS Snort dentro del Cuerpo de Bomberos de Babahoyo. Con diferentes estrategias se ha podido reunir información pertinente acerca de las funcionalidades, características y la efectividad de Snort en el análisis de las amenazas de la red dentro de la entidad.

Tabla 1. Comparación cuantitativa de amenazas antes y después de Snort

Métricas	**Antes de implementar Snort**	**Después de implementar Snort**	**Cambio**
Incidentes detectados	30/mes	75/mes	+150%
Faltos positivos	12/mes	4/mes	-67%
Falsos negativos	20/mes	7/mes	-65%
Tiempo de respuesta	3 horas	1 hora	-67%
Alertas Críticas	8/mes	25/mes	+213%
Numero de amenazas bloqueadas	15/mes	50/mes	+233%
Tasa de detección	50%	85%	+70%

Análisis: En el número de incidentes al implementar Snort aumenta por la capacidad que tiene para la identificación de amenazas en la red. En los falsos positivos hay una reducción de alertas incorrectas gracias a la configuración de Snort. Al igual que los falsos negativos hay una respuesta esperada debido a que Snort ayuda a identificar las amenazas que podrían pasar desapercibidas. Con el tiempo promedio de espera mejora al proporcionar alertas más precisas al implementar Snort. El número de alertar criticas aumenta al configurar Snort gracias a la detección que tiene ante este tipo de amenazas que antes no se podían identificar. Las amenazas bloqueadas aumentan debido a la identificación a tiempo real la cual evita que estas lleguen a causar daños. Logrando así la tasa de detección mejora con Snort ya que incrementa la porción de las amenazas detectadas respecto al total.

Durante las entrevistas semiestructuradas con el jefe del área de sistemas, se revelaron puntos de vista cruciales sobre la seguridad de la información. Se discutió cómo la implementación permanente de Snort podría mejorar significativamente esta área.

Las pruebas destacaron la capacidad de Snort para detectar actividades sospechosas de manera continua y alertar al equipo de sistemas sobre posibles amenazas.

Además, el análisis de las políticas de seguridad existentes y las configuraciones específicas de Snort arrojó luz sobre la alineación entre las necesidades de seguridad de la organización y las capacidades del sistema IDS. Se identificaron áreas de mejora y se ofrecieron recomendaciones para optimizar aún más la eficiencia y efectividad de Snort en el contexto operativo del Cuerpo de Bomberos de Babahoyo.

En resumen, los resultados de este estudio no solo ofrecen una visión detallada de la implementación práctica de Snort, sino que también proporcionan ideas significativas

sobre cómo esta tecnología puede fortalecer la seguridad cibernética de organizaciones similares en el sector público. Estos hallazgos son fundamentales para futuras informar decisiones estratégicas y mejoras continuas en la infraestructura de seguridad informática del Cuerpo de Bomberos de Babahoyo.

DISCUSIÓN DE RESULTADOS

La implementación de Snort como un IDS dentro del Cuerpo de Bomberos ha dado mejoras dentro de la seguridad de redes, como están en los resultados obtenidos. En la comparación de las métricas del antes y después de la implementación genera una visión mucho más clara del impacto que tiene en la protección de la infraestructura.

Teniendo en cuenta lo investigado se puede ver la importancia de conocer cada termino sobre todo como estos se manejan ya que al momento de configurar o poner las reglas establecidas es necesario saber cuáles son los que necesitamos para un mejor resultado. En la reducción de los falsos positivos y negativos nos da la referencia de que ha mejorado la detección de la calidad de intrusos. El anular las alertas incorrectas y enfocarse en las amenazas que antes no de detectaban ayudan a que el equipo de seguridad se enfoque en las amenazas que realmente generan gran impacto y de esa manera ganar tiempo.

Tener un promedio de respuesta más rápido indica mayor efectividad que tiene Snort al mejorar la manera en cómo la entidad organiza para eliminar las amenazas y gestionar de manera oportuna. Al tener una buena eficiencia operativa hace que el Cuerpo de Bombero logre un gran impacto en la seguridad de las operaciones diarias.

Al incrementar las alertas criticas también aumenta el número de amenazas bloqueadas lo que hace destacar nuevamente la capacidad de como Snort puede detectar de manera inmediata los ataques para poder prevenirlas de manera eficaz, lo que hace que Snort sea una herramienta con la fortaleza de mantener la disponibilidad y la integridad de la infraestructura tecnológica de esta entidad.

La implementación de Snort ha mejorado significativamente la seguridad de redes en el Cuerpo de Bomberos, como lo demuestran los datos obtenidos: los incidentes detectados aumentaron en un 150% (de 30 a 75 por mes), los falsos positivos se redujeron en un 67% (de 12 a 4 por mes) y los falsos negativos en un 65% (de 20 a 7 por mes). Además, el tiempo de respuesta disminuyó en un 67% (de 3 horas a 1 hora), las alertas críticas aumentaron en un 213% (de 8 a 25 por mes), las amenazas bloqueadas se incrementaron en un 233% (de 15 a 50 por mes) y la tasa de detección mejoró en un 70% (del 50% al 85%). Estos resultados reflejan una mayor capacidad de Snort para detectar y gestionar amenazas, mejorando la eficiencia operativa y la protección de la infraestructura tecnológica.

Con todo lo analizado, se refleja una gran mejora en la seguridad de la red, se puede validar el elevado nivel de protección, lo cual evidencia que Snort si puede ser una solución eficaz y confiable para tratar las amenazas cibernéticas actuales y a la vez futuras ya que si se ha fortalecido la integración para la protección de los activos digitales y la protección efectiva a los incidentes presentados.

CONCLUSIONES

La información recolectada fue valiosa sobre las herramientas existentes y las que el Cuerpo de Bombero necesitaba sobre la seguridad, lo que permitió la identificación de la necesidad de implementar un IDS como lo es Snort.

Se configuró las reglas necesarias en el Sistema de Identificación de Intrusos para la detección de ataques concurrentes, la cual mejora la protección de red debido a que se identifican con más rapidez los posibles ataques.

Con las pruebas y simulaciones de los ataques demostraron la efectividad de Snort en la detección de los ciberataques dentro de la red del cuerpo de bomberos.

RECOMENDACIONES

Se recomienda que se siga actualizando y ampliando conocimientos sobre las últimas tendencias sobre todo de las herramientas de seguridad para que la red se mantenga protegida.

Además, se sugiere que se continúe con las revisiones periódicas a las reglas personalizadas para que estén actualizadas y asegurarse que están adaptadas a las necesidades de cambio en la red.

Por último, se debe continuar realizando las pruebas y simulaciones regularmente para poder seguir evaluando la efectividad de Snort y de esa manera ajustar la configuración según sea necesario.

REFERENCIAS BIBLIOGRAFICAS

- Altube, R. (04 de mayo de 2023). *Open Webinars*. Obtenido de https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/
- Asenjo, S. (17 de julio de 2024). *Xatak Android*. Obtenido de https://www.xatakandroid.com/aplicaciones-android/mejores-vpn-para-android-cual-elegir-funcion-tus-necesidades
- *Atico*. (07 de marzo de 2021). Obtenido de https://protecciondatos-lopd.com/empresas/Snort-deteccion-intrusos/
- Belcic, I. (22 de septiembre de 2020). *Avast*. Obtenido de https://www.avast.com/es-es/c-sql-injection
- Belcic, I. (19 de enero de 2023). *Avast*. Obtenido de https://www.avast.com/es-es/c-malware
- Chavarría, J. (19 de diciembre de 2023). *fluidattacks*. Obtenido de https://fluidattacks.com/es/blog/pentesting/
- Cilleruelo, C. (11 de julio de 2024). *Keepcoding*. Obtenido de https://keepcoding.io/blog/fases-de-un-test-de-intrusion/
- Dominguez, S. (13 de octubre de 2023). *openwebinars*. Obtenido de https://openwebinars.net/blog/los-15-tipos-de-ciberataques-que-deberias-conocer/
- Escalante, M. (08 de junio de 2023). *Abc Xperts*. Obtenido de https://abcxperts.com/que-es-un-sistema-de-prevencion-de-intrusiones-ips/?utm_campaign=que-es-un-sistema-de-prevencion-de-intrusiones-ips&utm_medium=rss&utm_source=rss

- Escalante, M. (27 de junio de 2023). *Abcxperts*. Obtenido de https://abcxperts.com/que-es-un-sistema-de-deteccion-de-intrusiones-ids/
- Fisher, S. (30 de julio de 2019). *Avast*. Obtenido de https://www.avast.com/es-es/c-what-is-tcp-ip
- Flores, J. (15 de diciembre de 2022). *National Geographic*. Obtenido de https://www.nationalgeographic.com.es/ciencia/que-es-5g-y-como-nos-cambiara-vida_14449
- Gillis, A. S. (25 de agosto de 2021). *Computer Weekly*. Obtenido de https://www.computerweekly.com/es/definicion/Red-privada-virtual-o-VPN
- *Global Suite Solutions*. (20 de marzo de 2023). Obtenido de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/
- Gómez, J. A. (6 de mayo de 2024). *delta*. Obtenido de https://www.deltaprotect.com/blog/tipos-de-firewall
- Gómez, J. A. (6 de mayo de 2024). *Delta*. Obtenido de https://www.deltaprotect.com/blog/tipos-de-firewall
- *Kaspersky*. (23 de noviembre de 2021). Obtenido de https://latam.kaspersky.com/resource-center/threats/ddos-attacks
- Limones, E. (17 de septiembre de 2021). *Open Webinars*. Obtenido de https://openwebinars.net/blog/protocolo-de-red-que-es-tipos-y-caracteristicas/
- Micucci, M. (10 de enero de 2024). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/es/seguridad-corporativa/vulnerabilidades-mas-relevantes-2023/

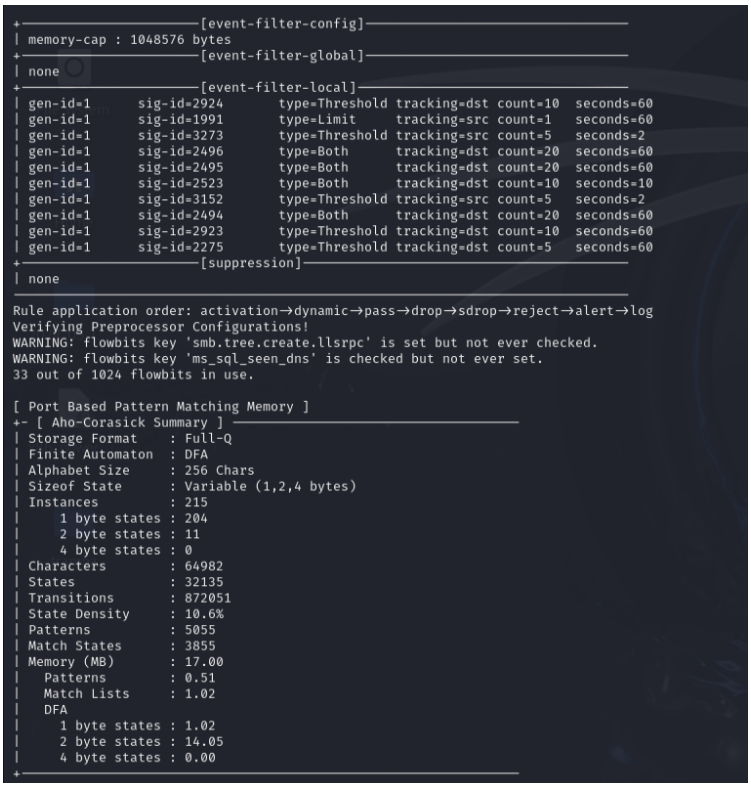
- Santos Chavez, J. J. (22 de mayo de 2024). *delta*. Obtenido de https://www.deltaprotect.com/blog/seguridad-para-base-de-datos
- Serra, J. (02 de febrero de 2023). *Ciberseguridad*. Obtenido de https://ciberseguridadtips.com/que-es-eset-nod32/

ANEXOS

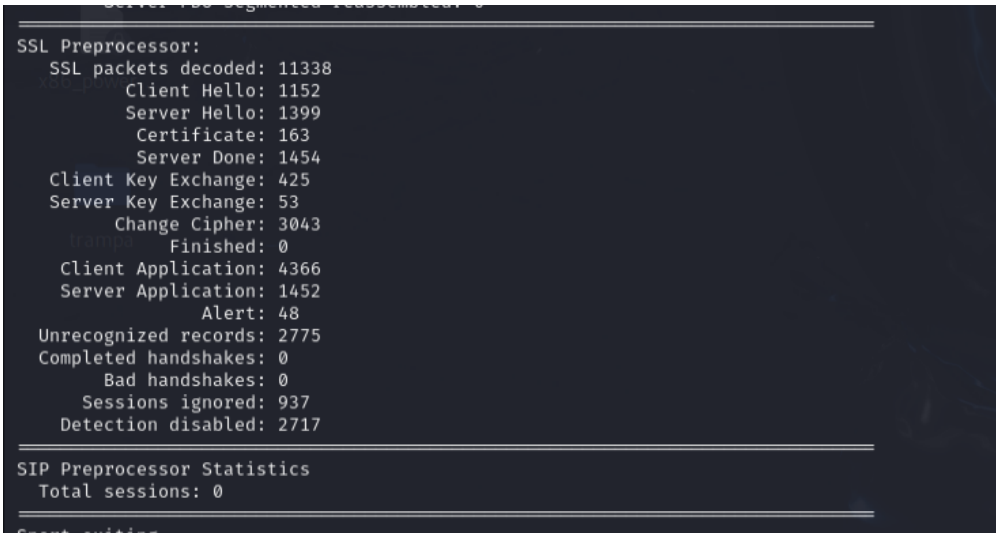
```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
Commencing packet processing (pid=4862)

^C
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 29063.387210 seconds
Snort processed 531714 packets.
Snort ran for 0 days 8 hours 4 minutes 23 seconds
    Pkts/hr:        66464
   Pkts/min:         1098
   Pkts/sec:           18
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       45051904
  Bytes in mapped regions (hblkhd):      13574144
  Total allocated space (uordblks):      40418688
  Total free space (fordblks):           4633216
  Topmost releasable block (keepcost):   83936
```

```
===============================================================================
Frag3 statistics:
         Total Fragments: 32
      Frags Reassembled: 16
               Discards: 0
        Memory Faults: 0
              Timeouts: 0
              Overlaps: 0
            Anomalies: 0
               Alerts: 0
                Drops: 0
    FragTrackers Added: 16
   FragTrackers Dumped: 16
FragTrackers Auto Freed: 0
   Frag Nodes Inserted: 32
    Frag Nodes Deleted: 32
===============================================================================
===============================================================================
Stream statistics:
           Total sessions: 9441
             TCP sessions: 1654
             UDP sessions: 7787
            ICMP sessions: 0
              IP sessions: 0
               TCP Prunes: 0
               UDP Prunes: 0
              ICMP Prunes: 0
                IP Prunes: 0
TCP StreamTrackers Created: 1654
TCP StreamTrackers Deleted: 1654
              TCP Timeouts: 14
              TCP Overlaps: 10
      TCP Segments Queued: 6550
    TCP Segments Released: 6550
      TCP Rebuilt Packets: 3868
       TCP Segments Used: 5086
           TCP Discards: 2065
                TCP Gaps: 1288
     UDP Sessions Created: 7980
     UDP Sessions Deleted: 7980
             UDP Timeouts: 193
             UDP Discards: 0
                   Events: 5131
          Internal Events: 0
          TCP Port Filter
                 Filtered: 0
                Inspected: 0
                  Tracked: 57538
          UDP Port Filter
                 Filtered: 0
                Inspected: 0
                  Tracked: 7787
===============================================================================
```

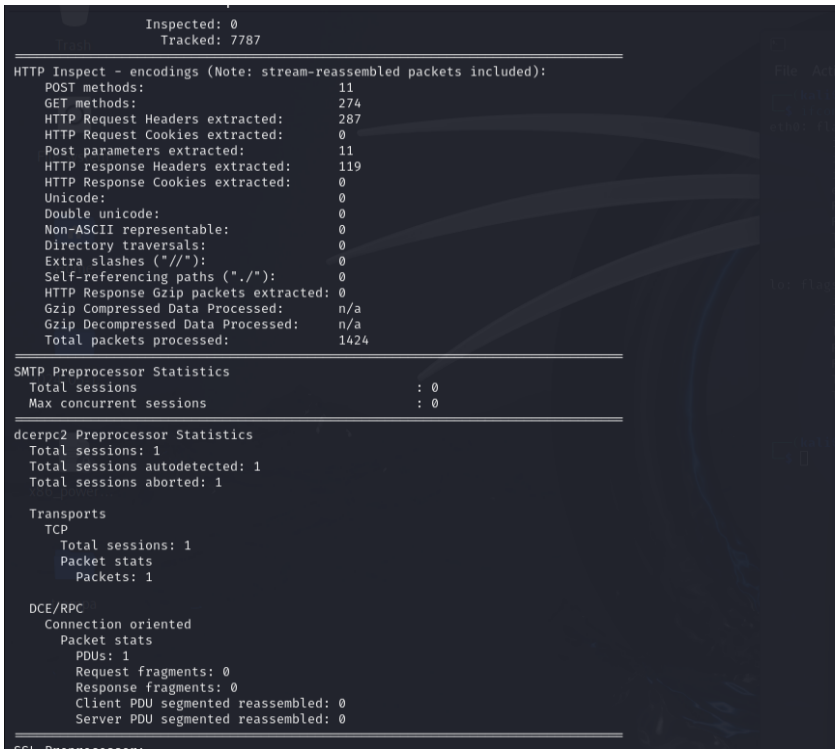
```
     Teredo:            0 (  0.000%)
    ICMP-IP:          455 (  0.086%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:         4579 (  0.861%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:         6942 (  1.305%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:         6942 (  1.305%)
      Other:         1693 (  0.318%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:           29 (  0.005%)
     S5 G 2:           28 (  0.005%)
      Total:       531787
===============================================================================
Action Stats:
     Alerts:          112 (  0.021%)
     Logged:          112 (  0.021%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:       494543 ( 93.008%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:        37171 (  6.991%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)
===============================================================================
```



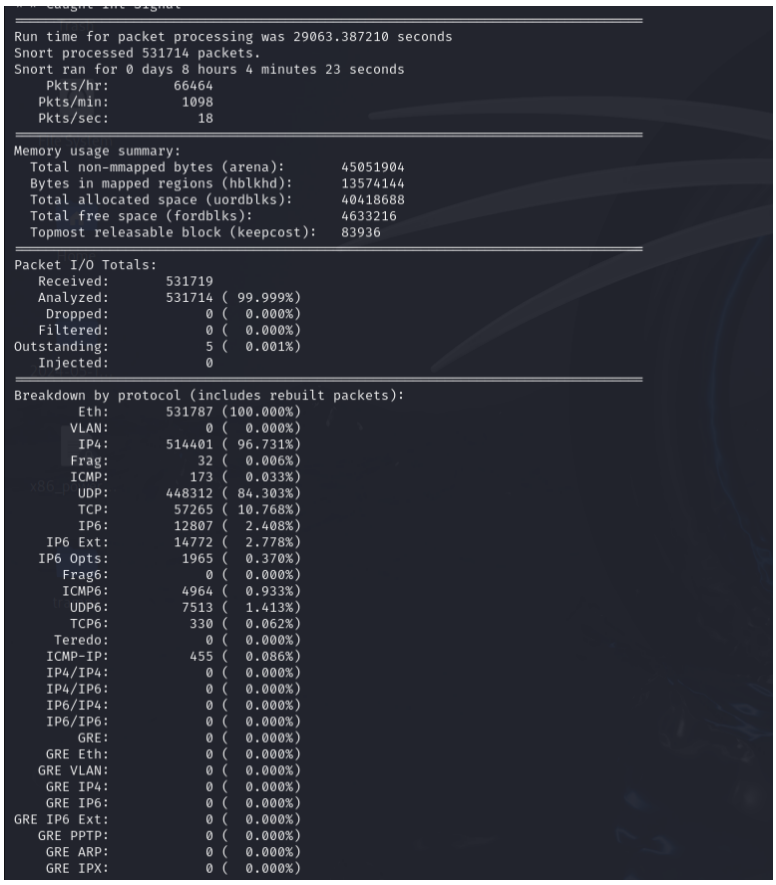
```
+----------------------[event-filter-config]---------------------------------
| memory-cap : 1048576 bytes
+----------------------[event-filter-global]---------------------------------
| none
+----------------------[event-filter-local]----------------------------------
| gen-id=1      sig-id=2924       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=1991       type=Limit     tracking=src count=1   seconds=60
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2496       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2495       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=10
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2494       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2275       type=Threshold tracking=dst count=5   seconds=60
+----------------------[suppression]----------------------------------------
| none
-------------------------------------------------------------------------------
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'smb.tree.create.llsrpc' is set but not ever checked.
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
33 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] ------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64982
| States            : 32135
| Transitions       : 872051
| State Density     : 10.6%
| Patterns          : 5055
| Match States      : 3855
| Memory (MB)       : 17.00
|   Patterns        : 0.51
|   Match Lists     : 1.02
|   DFA
|     1 byte states : 1.02
|     2 byte states : 14.05
|     4 byte states : 0.00
+--------------------------------------------------------------------
```



```
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 11338
           Client Hello: 1152
           Server Hello: 1399
            Certificate: 163
            Server Done: 1454
   Client Key Exchange: 425
   Server Key Exchange: 53
         Change Cipher: 3043
              Finished: 0
    Client Application: 4366
    Server Application: 1452
                 Alert: 48
  Unrecognized records: 2775
  Completed handshakes: 0
        Bad handshakes: 0
      Sessions ignored: 937
    Detection disabled: 2717
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
```



```
               Inspected: 0
                 Tracked: 7787
===================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         11
    GET methods:                          274
    HTTP Request Headers extracted:       287
    HTTP Request Cookies extracted:       0
    Post parameters extracted:            11
    HTTP response Headers extracted:      119
    HTTP Response Cookies extracted:      0
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 0
    Self-referencing paths ("./"):        0
    HTTP Response Gzip packets extracted: 0
    Gzip Compressed Data Processed:       n/a
    Gzip Decompressed Data Processed:     n/a
    Total packets processed:              1424
===================================================================
SMTP Preprocessor Statistics
  Total sessions                                : 0
  Max concurrent sessions                       : 0
===================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 1
  Total sessions autodetected: 1
  Total sessions aborted: 1

  Transports
    TCP
      Total sessions: 1
      Packet stats
        Packets: 1

  DCE/RPC
    Connection oriented
      Packet stats
        PDUs: 1
        Request fragments: 0
        Response fragments: 0
        Client PDU segmented reassembled: 0
        Server PDU segmented reassembled: 0
===================================================================
```



```
===================================================================
Run time for packet processing was 29063.387210 seconds
Snort processed 531714 packets.
Snort ran for 0 days 8 hours 4 minutes 23 seconds
    Pkts/hr:        66464
   Pkts/min:         1098
   Pkts/sec:           18
===================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       45051904
  Bytes in mapped regions (hblkhd):      13574144
  Total allocated space (uordblks):      40418688
  Total free space (fordblks):           4633216
  Topmost releasable block (keepcost):   83936
===================================================================
Packet I/O Totals:
   Received:       531719
   Analyzed:       531714 ( 99.999%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            5 (  0.001%)
   Injected:            0
===================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:       531787 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:       514401 ( 96.731%)
       Frag:           32 (  0.006%)
       ICMP:          173 (  0.033%)
        UDP:       448312 ( 84.303%)
        TCP:        57265 ( 10.768%)
        IP6:        12807 (  2.408%)
    IP6 Ext:        14772 (  2.778%)
   IP6 Opts:         1965 (  0.370%)
      Frag6:            0 (  0.000%)
      ICMP6:         4964 (  0.933%)
       UDP6:         7513 (  1.413%)
       TCP6:          330 (  0.062%)
     Teredo:            0 (  0.000%)
    ICMP-IP:          455 (  0.086%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
```