CARRERA: TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES

TEMA:

“IMPLEMENTACIÓN DE LA HERRAMIENTA DE SEGURIDAD SURICATA EN MICROEMPRESAS CON ENDPOINTs BASADOS EN ARQUITECTURA WINDOWS Y LINUX”

Proyecto Integrador de grado previo a la obtención del título de Tecnólogo Superior en Redes & Telecomunicaciones

AUTOR: JONATHAN STEVE MEJÍA MÉNDEZ

DIRECTOR: ING. CHRISTIAN LEONARDO BONILLA MORALES MSC.

D.M. Quito,07 de Febrero del 2023.

DEDICATORIA

El presente trabajo investigativo lo dedico principalmente a mi señora madre, por ser la persona que me inspiro a salir a delante dándome la fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

AGRADECIMIENTO

Me gustaría agradecer en estas líneas la ayuda de muchas personas y colegas que me han prestado su tiempo durante el proceso de investigación y redacción de este trabajo.

En primer lugar, quisiera agradecer a mi señora madre por el esfuerzo, paciencia por su confianza, ayudada y apoyo a lo largo de toda mi carrera, a mi tutor, MSc. Christian Bonilla, por haberme orientado en todos los momentos que necesite sus consejos.

AUTORIA

Yo, JONATHAN STEVE MEJÍA MÉNDEZ autor del presente informe, me responsabilizo por los conceptos, opiniones y propuestas contenidos en el mismo.

Atentamente,

Jonathan Steve Mejía Méndez

D.M. Quito, 07 de Febrero del 2023.

ING. CHRISTIAN LEONARDO BONILLA MORALES MSC.

DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICA

Haber revisado el presente informe de investigación, que se ajusta a las normas institucionales y académicas establecidas por el Instituto Tecnológico Superior Internacional ITI, de Quito, por tanto, se autoriza su presentación final para los fines legales pertinentes.

_____

Ing. Christian Leonardo Bonilla Morales MSc.

D.M. Quito, 07 de Febrero del 2023.

DECLARACIÓN DE CESIÓN DE DERECHOS DE TRABAJO FIN DE CARRERA

Yo, Jonathan Steve Mejía Méndez, declaro ser autor del Trabajo de Investigación con el nombre "IMPLEMENTACIÓN DE LA HERRAMIENTA DE SEGURIDAD SURICATA EN MICROEMPRESAS CON ENDPOINTs BASADOS EN ARQUITECTURA WINDOWS", como requisito para optar al grado de Tecnólogo Superior en Redes & Telecomunicaciones y autorizo al Sistema de Bibliotecas del Instituto Tecnológico Superior Internacional Universitario, para que con fines netamente académicos divulgue esta obra a través del Repositorio Digital Institucional (RDI-ITI).

Los usuarios del RDI-ITI podrán consultar el contenido de este trabajo en las redes de información del país y del exterior, con las cuales la Universidad tenga convenios. El Instituto Tecnológico Internacional Universitario, no se hace responsable por el plagio o copia del contenido parcial o total de este trabajo.

Del mismo modo, acepto que los Derechos de Autor, Morales y Patrimoniales, sobre esta obra, serán compartidos entre mi persona y el Instituto Tecnológico Internacional Universitario, y que no tramitaré la publicación de esta obra en ningún otro medio, sin autorización expresa de la misma. En caso de que exista el potencial de generación de beneficios económicos o patentes, producto de este trabajo, acepto que se deberán firmar convenios específicos adicionales, donde se acuerden los términos de adjudicación de dichos beneficios.

Para constancia de esta autorización, en la ciudad de Quito, a los 30 días del mes de Enero de 2023, firmo conforme: Conste por el presente documento la cesión de los derechos en trabajo fin de carrera, de conformidad con las siguientes clausulas:

PRIMERA: El Ing. Christian Leonardo Bonilla Morales MSc. y por sus propios derechos en calidad de Director del trabajo fin de carrera; y el Sr. Jonathan Steve Mejía Méndez por sus propios derechos, en calidad de autor del trabajo fin de carrera.

SEGUNDA:
UNO.- El Sr. Jonathan Steve Mejía Méndez realizó el trabajo fin de carrera titulado: **IMPLEMENTACIÓN DE LA HERRAMIENTA DE SEGURIDAD SURICATA EN MICROEMPRESAS CON ENDPOINTs BASADOS EN ARQUITECTURA WINDOWS,** para optar por el título de, **Tecnólogo Superior en Redes y Telecomunicaciones** en el Instituto Tecnológico Superior Internacional ITI, bajo la dirección de Ing. Christian Leonardo Bonilla Morales MSc.
DOS.- Es política del Instituto Tecnológico Superior Internacional ITI, que los trabajos fin de carrera se aplique, se materialicen y difundan en beneficio de la comunidad.
TRES: Los comparecientes, Ing. Christian Leonardo Bonilla Morales MSc., en calidad de director del trabajo fin de carrera y el Sr. Jonathan Steve Mejía Méndez, como autora del mismo, por medio del presente instrumento, tienen a bien ceder en

forma gratuita sus derechos en el trabajo fin de Carrera titulado: **IMPLEMENTACIÓN DE LA HERRAMIENTA DE SEGURIDAD SURICATA EN MICROEMPRESAS CON ENDPOINTs BASADOS EN ARQUITECTURA WINDOWS,** y conceden autorización para que el ITI pueda utilizar este trabajo en su beneficio y/o de la comunidad, sin reserva alguna.

CUARTA: aceptación: las partes declaradas que aceptan expresamente todo lo estipulado en la presente cesión de derecho.

_____

Ing. Christian Leonardo Bonilla Morales MSc.

_____

Sr. Jonathan Steve Mejía Méndez

D.M. Quito, 07 de Febrero del 2023.

ÍNDICE

ÍNDICE 8
ÍNDICE DE TABLAS 11
ÍNDICE DE FIGURAS 12
RESUMEN 16
INTRODUCCIÓN 17
Nombre del proyecto 17
Antecedentes 17
Marco contextual 18
Análisis macro 18
Análisis meso 21
Análisis micro 22
Problema de investigación 22
Definición del problema 22
Idea a defender 23
Objetivo de estudio y campo de acción 25
Objeto de estudio: 25
Campo de acción: 25
Justificación 25
Objetivos 26
General 26
Específicos 26
Síntesis de la introducción 27
CAPÍTULO I: FUNDAMENTACIÓN TEÓRICA 28
Antecedentes históricos 28

Análisis de la zona de estudio 40
Fundamentación Conceptual 41
Fundamentación Legal 42
Fundamentación Técnica y/o Tecnológica 44
Suricata 45
Síntesis del capítulo 45
CAPÍTULO II: DIAGNÓSTICO 46
Tipos de investigación 46
Métodos de investigación 46
Técnicas e instrumentos de investigación 47
Universo y muestra 48
Universo: 48
Muestra: 48
Fórmula establecida 49
Presentación gráfica, análisis e interpretación de resultados obtenidos 51
Análisis e interpretación de resultados 54
Síntesis del capítulo 55
CAPÍTULO III: PROPUESTA 56
Descripción de la propuesta 56
Viabilidad 56
Impacto 56
Desarrollo de la propuesta 57
Síntesis del capítulo 86
CAPÍTULO IV: ESFUERZO PARA LA PERSONALIZACIÓN DE SURICATA 87
Análisis 87

Alcance: primera fase de pruebas 87
Cálculo hora especializada 87
Documentación 89
Cálculo de presupuesto 89
Tipos de clientes: 90
Empresa pequeña 90
Empresa mediana 90
Empresa grande 90
Síntesis del capítulo 91
CONCLUSIONES 92
RECOMENDACIONES 94
REFERENCIAS BIBLIOGRÁFICAS 95
ANEXOS 99

ÍNDICE DE TABLAS

Tabla 1: Informe sobre el número de empresas por tamaño de empresa 2012-2020. 19
Tabla 2: Informe sobre el número de empresas por tamaño de empresa 2020. 20
Tabla 3: Tabla de composición de las reglas de SURICATA. 70
Tabla 4: Tabla de formato de las reglas de SURICATA. 70
Tabla 5: Tabla de los diferentes tipos de empresas. 89

ÍNDICE DE FIGURAS

Figura 1: Estructura sectorial de Número de empresas, subcategoría Tamaño de empresas. 24
Figura 2: Informe sobre el ransomware en pequeñas y medianas empresas. 26
Figura 3: Países de Latinoamérica vs ataques informáticos. 30
Figura 4: Mapa en tiempo real de ataques cibernéticos. 32
Figura 5: Estadísticas del top de amenazas más frecuentes en el Ecuador por volumen. 33
Figura 6: Exploit: Win32/CVE-2017-11882. 35
Figura 7: Actualización de firmware 2022-08-02 Google Chrome. 35
Figura 8: Top tipo de industrias más afectadas. 36
Figura 9: Estadísticas del top de amenazas más frecuentes en el Ecuador por equipo. 37
Figura 10: Ubicación empresa T&M Technology. 40
Figura 11: Topología de la red con Suricata. 44
Figura 12: Análisis de Riesgos a la Seguridad Nacional 2021-2023. 47
Figura 13: Estructura sectorial de número de empresas, subcategoría, tamaño de empresas. 49
Figura 14: Encuesta Pregunta 1. 51
Figura 15: Encuesta Pregunta 2. 51
Figura 16: Encuesta Pregunta 4. 52
Figura 17: Encuesta Pregunta 7. 52
Figura 18: Encuesta Pregunta 8. 53
Figura 19: Encuesta Pregunta 9. 53
Figura 20: Encuesta Pregunta 10. 54
Figura 21: Actualización de los repositorios de Ubuntu Server 22.04. 57
Figura 22: Escalamiento de privilegios. 58
Figura 23: Instalación de la herramienta de seguridad SURICATA. 58
Figura 24: Actualización de los paquetes del sistema. 60
Figura 25: Instalación de los repositorios de SURICATA y SURICATA JQ. 60

Figura 26: Confirmación de la instalación exitosa de SURICATA con un “Donde esta”..... 62
Figura 27: Validación de que SURICATA este activo y que los servicios más importantes en especial NFQueue estén corriendo..... 62
Figura 28: Búsqueda del fichero que contiene las reglas de SURICATA en el directorio /etc/suricata..... 64
Figura 29: Revisión del fichero suricata.yaml, donde se realizaran las configuraciones de las nuevas reglas y directorios..... 65
Figura 30: Revisión del fichero suricata.yaml, donde se realizaran las configuraciones de las nuevas reglas y directorios..... 65
Figura 31: Validación del directorio donde se encuentra albergado los logs de SURICATA..... 66
Figura 32: Comprobación de la interfaz de red por donde se va a comunicar SURICATA..... 67
Figura 33: Comprobación de la interfaz de red..... 67
Figura 34: Comprobación del estatus de los protocolos en SURICATA..... 68
Figura 35: Listado de los ficheros de SURICATA albergados dentro del directorio /etc/suricata/rules..... 69
Figura 36: Lectura del fichero dhcp-events.rules..... 69
Figura 37: Creación de un nuevo fichero membretado my.rules..... 71
Figura 38: Validación de las rutas existentes dentro del archivo de configuración general..... 72
Figura 39: Cambio del directorio anterior al nuevo en donde se encuentra el archivo creado anteriormente..... 72
Figura 40: Cambio del nombre del fichero anterior por el que se ha creado..... 73
Figura 41: Creación de la primera regla dentro del fichero my.rules..... 73
Figura 42: Puesta en marcha del servicio de SURICATA..... 73
Figura 43: Revisión de los logs registrados por incidencias dentro de la red..... 74
Figura 44: Realización de un ICMP o ping exitoso, desde la maquina atacante..... 74
Figura 45: Revisión de las alertas en el fichero fast.log por un ping enviado desde una máquina..... 74
Figura 46: Creación de las reglas para el bloqueo de redes sociales..... 75

Figura 47: Mediante curl -i se valida la conexión a las redes sociales. 75
Figura 48: Revisión en el fichero fast.log. 75
Figura 49: Creación de la regla para peticiones get. 76
Figura 50: Mediante curl -i se valida la petición a un servicio en la web. 76
Figura 51: Comprobación del correcto funcionamiento de la regla en el fichero fast.log 76
Figura 52: Creación de la regla para conexiones SSH. 77
Figura 53: Conexión hacia el servidor Ubuntu 22.04 mediante PuTTY. 77
Figura 54: Comprobación del correcto funcionamiento de la regla en el fichero fast.log 77
Figura 55: Creación de la regla para detección de un escaneo de puertos. 78
Figura 56: Escaneo de puertos desde la maquina atacante mediante NMAP. 78
Figura 57: Comprobación del correcto funcionamiento de la regla en el fichero fast.log 78
Figura 58: Listado de los registros de los ficheros en formato JSON. 79
Figura 59: Lectura de un fichero en formato JSON. 79
Figura 60: Instalación de la herramienta JQ. 79
Figura 61: Lectura del fichero **eve.json** mediante la herramienta JQ. 80
Figura 62: Validación de los 10 puertos más usados con la herramienta JQ. 81
Figura 63: Verificación de que **NFQueue** este activado. 81
Figura 64: Revisión de las IPTABLES propias de Ubuntu server 22.04. 82
Figura 65: Configuración de las IPTABLES “forward” y redireccionamiento hacia SURICATA. 82
Figura 66: Configuración de las IPTABLES “input, output” y redireccionamiento hacia SURICATA. 83
Figura 67: Configuración de las reglas creadas en los pasos anteriores. 83
Figura 68: Actualización de los repositorios de SURICATA. 84
Figura 69: Revisión de las reglas por defecto que tiene SURICATA. 85
Figura 70: Configuración del fichero suricata.yaml, inserción del nuevo directorio y archivo. 85
Figura 71: Que es Suricata. 99
Figura 72: Integración con terceros. 100

Figura 73: Licencias... 103

RESUMEN

En la actualidad el Ecuador presenta inmensas falencias en cuestión de seguridad cibernética lo cual conlleva a que las empresas sean un blanco fácil ante los ciber delincuentes, dado que existen varias maneras de vulnerar una red por ataques de pishing, ingeniería social, ataques de fuerza bruta entre otros, por medio de la presente investigación se intenta demostrar la forma más idónea que las empresas pueden aplicar para defenderse y contrarrestar los ataques que pueden llegar a sufrir, por medio del método analítico se va a dar un vistazo tanto de las partes poblacionales como empresariales del ecuador observando como el país es consciente de esta problemática y cuáles son las acciones tomadas para mitigar dicho problema, demostrando así la importancia de implementar una herramienta de seguridad en las redes empresariales como lo es SURICATA ya que esta tiene la facilidad de ser un IDS/IPS y le permite monitorear cualquier anomalía en la red de transmisión de datos corporativa.

Palabras claves:

- **Suricata, Seguridad, Hackers, Redes, Crackers.**

INTRODUCCIÓN

Nombre del proyecto

“IMPLEMENTACIÓN DE LA HERRAMIENTA DE SEGURIDAD SURICATA EN MICROEMPRESAS DE LA CUIDAD DE QUITO CON ENDPOINTs BASADOS EN ARQUITECTURA WINDOWS & LINUX”

Antecedentes

Internet se ha convertido en una parte indispensable en nuestra cotidianeidad a tal punto que tipo de organizaciones, como instituciones médicas, financieras y educativas, utilizan esta red para funcionar de manera efectiva. Utilizan redes para recopilar, procesar, almacenar y compartir grandes cantidades de información digital. A medida que se recopila, difunde información digital, proteger se vuelve cada vez más importante para nuestra seguridad nacional y estabilidad económica.

"La ciberseguridad es el esfuerzo continuo para proteger el sistema de red y todos los datos del uso no autorizado o la corrupción".(Cisco, 2022b). Las Microempresas, son entidades que por el mismo hecho de asumirse como pequeñas, se consideran exentas de ser atacadas, mientras tanto la realidad muestra lo contrario. p.ej., “Según el último informe anual realizado por la compañía de antivirus Kaspersky muestra que hay un aumento del 75% en los ataques informáticos en Ecuador, lo que significa que hay 89 ataques por minuto.”(Ortiz, 2021).

Además, Galo Cárdenas, Máster en Ciencias Informáticas y Profesor de la Universidad Internacional SEK (UISEK), señala que son muchas las herramientas a las que tienen acceso las pymes para proteger su información. Según él, para

garantizar la seguridad de los datos medianos se requiere una inversión de al menos $ 1.700 por máquina, el 70% de los ataques a las empresas sean estas pequeñas y medianas son malware a través de phishing o robo de identidad.(Ortiz, 2021).

En consecuencia, es menester la aplicación de herramientas de seguridad y no solo amolarse con la instalación de Antivirus (Anti-Malware) mismos que en muchos casos no constan con licencias originales, si no con keygen[1]; los cuales pueden llegar a ser troyanos o rootkits dejando así una puerta trasera en los sistemas operativos, los cuales no son detectables ni con los firewalls propios del sistema operativo ya que estos son instalados a nivel de terminal (Shell, Bash) y se instalan como propios del sistema, todo esto causa daños irreversibles a las empresas, por este motivo, se incluye una herramienta de seguridad adicional que mejorará en gran medida la protección de la red empresarial de las Microempresas en las cuales se encuentren alojadas.

Marco contextual

Análisis macro

En un mundo en el que se puede evidenciar como emerge en la cotidianidad tanto las vulnerabilidades de software como las vulnerabilidades de hardware, p.ej. “En 2015, se descubrió una vulnerabilidad crítica llamada SYNful Knock en Cisco IOS. Estas vulnerabilidades podrían permitir que un atacante tome el control de los

[1] Keygen (del inglés key generator, generador de claves) es un programa informático que, al ejecutarse, genera código para que un determinado programa de pago en versión de prueba (Shareware) pueda proporcionar todo el contenido del programa. Por lo general, los generadores de claves son archivos ejecutables (en formato *.exe) que se ejecutan sin instalación. Tomado de https://es-academic.com/dic.nsf/eswiki/679835

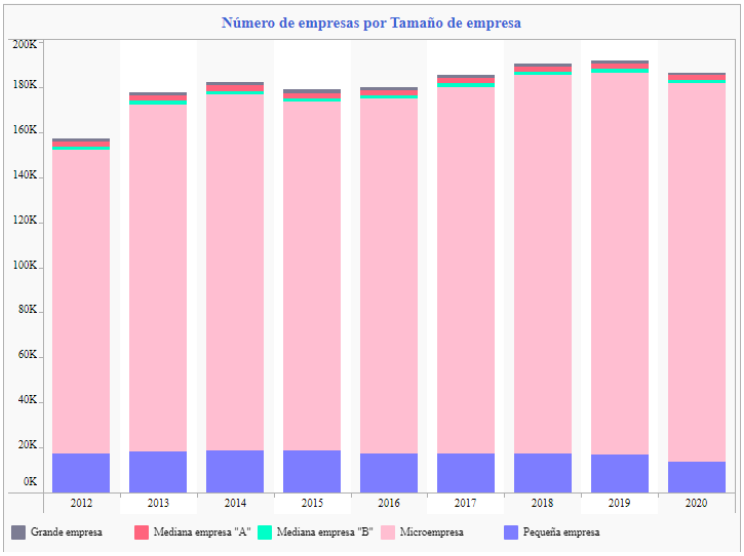
enrutadores empresariales, como los enrutadores heredados Cisco 1841, 2811 y 3825.”(Cisco, 2022a).

La mayoría de las vulnerabilidades de software son explotadas por ciberdelincuentes que usan herramientas como Metasploit, Nmap, Medusa y otras, así como malware como Spyware, Ransomware, Rootkits y otras para tener acceso a la red de la víctima. facilitar la interceptación, por lo que las microempresas se ven en la necesidad de implementar medidas más estrictas, como implementar más medidas de seguridad, para poder contrarrestar dichas amenazas.

No obstante, el Ecuador no está exento de este problema global, por los ataques dados a compañías del país como bancos, de telecomunicación, etc.... Dichas compañías han sido grandes empresas sobre todo las microempresas no son inmunes a los ataques cibernéticos.

Tabla 1:

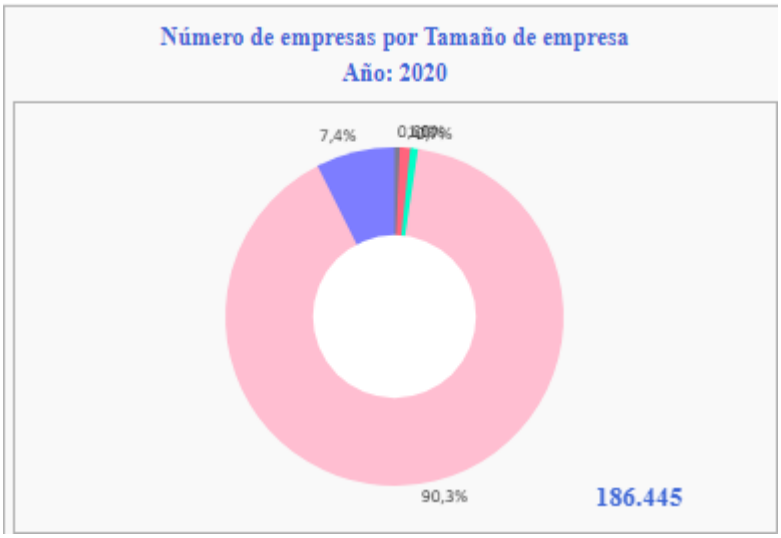
Informe sobre el número de empresas por tamaño de empresa 2012-2020.



Fuente: (INEC, 2022b)

Se ha escogido el rango de las microempresas ya que según los datos estadísticos del Instituto Nacional de Estadística y Censos (en adelante INEC), indica que el rango más amplio de empresas a lo largo de casi una década son las microempresas, como se indica en la Tabla 1, este tipo de empresas utilizan como programas para bases de datos y estadísticas la herramienta Excel de Microsoft Office, adicional a esto este tipo de empresas consta con una logística muy básica que es dirigidas por ellos mismos (los dueños - emprendedores), ya que como se explica en las estadísticas de la SuperCias[2] las microempresas constan a penas de 1-2 trabajadores en total, haciendo que ellos manejen absolutamente todo los movimientos (todas las áreas) de la empresa incluyendo el departamento de sistemas; el mismo que no existe de una forma adecuada.

Tabla 2:
Informe sobre el número de empresas por tamaño de empresa 2020.



Fuente: (INEC, 2022b)

[2] La Superintendencia de Compañías, Valores y es un órgano técnico con autonomía administrativa y económica que controla y supervisa la organización, funcionamiento, funcionamiento, disolución y liquidación de las sociedades y demás organizaciones en los casos y en las condiciones que determine la ley. Tomado de https://www.supercias.gob.ec/portalscvs/Institucion.php

Se ha escogido el rango de las microempresas porque forman un 90,3% de todas las empresas a nivel Quito-Pichincha-Ecuador con un total de 186.445 empresas, de acuerdo a la Tabla 2, este tipo de empresas no utilizan herramientas o programas para manejar una base de datos o estadísticas como lo hacen el resto de empresas (PyMes) ya que no cuentan con una infraestructura y con un personal el cual sea capacitado para el manejo de dichas plataformas, las microempresas por motivos de falta de una constitución empresarial hace que solo los propios dueños efectúen las funciones de los perfiles como: jefe, sistemas, jefe de logística, cajero, etc. Realizan todas las tareas a base de un programa o máximo dos que es Excel, para estadísticas, inventario y el segundo que es el manejo de su propio vehículo o uso de aplicativos como lo son UBER para el manejo del reparto de sus productos.

Por este hecho que se evidencia dentro de nuestro país y a nivel mundial, es estrictamente necesario una implementación de herramientas de seguridad como son IDS, IPS O SIEM, las cuales brindan un mejor monitoreo en hosts y red evitando así las brechas de seguridad que se puede generar por un mal uso o una mala práctica de la triada C.I.D, dentro de las medianas, pequeñas y microempresas, siendo estas últimas las microempresas, utilizan una red local del domicilio para conectarse a internet y realizar sus actividades empresariales poniendo así en peligro la integridad de los datos no solo corporativos si no personales ya que no diferencian de dispositivos y mucho menos de las autenticaciones.

Análisis meso

Por medio de la presente investigación se puede llegar a solventar una brecha de seguridad que presentan las redes de las Microempresas, evitando y

ayudando, a que no se vean comprometidos los datos que se manejan en los dispositivos.

Análisis micro

Instalación dentro de los equipos ya sean estos de escritorio o portables (laptops) la instalación del software SURICATA, este software le permite monitorear dispositivos en su red ya que es una combinación del Sistema de Detección de Intrusos (IDS); sistema de prevención de intrusiones (IPS); Monitoreo de seguridad de red (NSM) y manejo (PCAP), gracias a esto y por medio de la herramienta de monitorización en tiempo real que nos ofrece este software, permite así detecciones tempranas de fallas o ataques sofisticados que pueden presentarse en la red y dispositivos, el cual nos indica con una alerta de los ataques y se procede al bloqueo de los malwares automáticamente. No obstante, para analizar dicho comportamiento se procederá a realizar ataques a la red y a los dispositivos conectados en la misma mediante un dispositivo móvil con KALI NETHUNTER nativo.

Problema de investigación

Definición del problema

“Ecuador tiene brechas significativas en la identificación de amenazas y la inacción de las agencias regulwdadoras, y mucho menos en la planificación para responder a los ataques de información”(Alvarado Chang, 2020); Los constantes ataques que se han presentado en el país a todo tipo de Microempresas, han sido motivo de preocupación y malestar para los propietarios de las mismas ya que un ataque cibernético conlleva no solo la caída del servicio sino también de la

denegación de acceso al servicio la cual se ha representado en perdidas cuantitativas para las empresas que sufren o han sufrido un ataque.

El descuido de no priorizar algo tan importante como es el cuidado de los datos; la carencia de un departamento de seguridad cibernética, constar con personal calificado o con la aplicación de protocolos de seguridad dentro de las empresas ha sido uno de los grandes problemas de inseguridad a la microempresa ya que consideran un gasto innecesario la implementación de seguridades, dejando así de lado a una parte vital para el funcionamiento adecuado de la red.

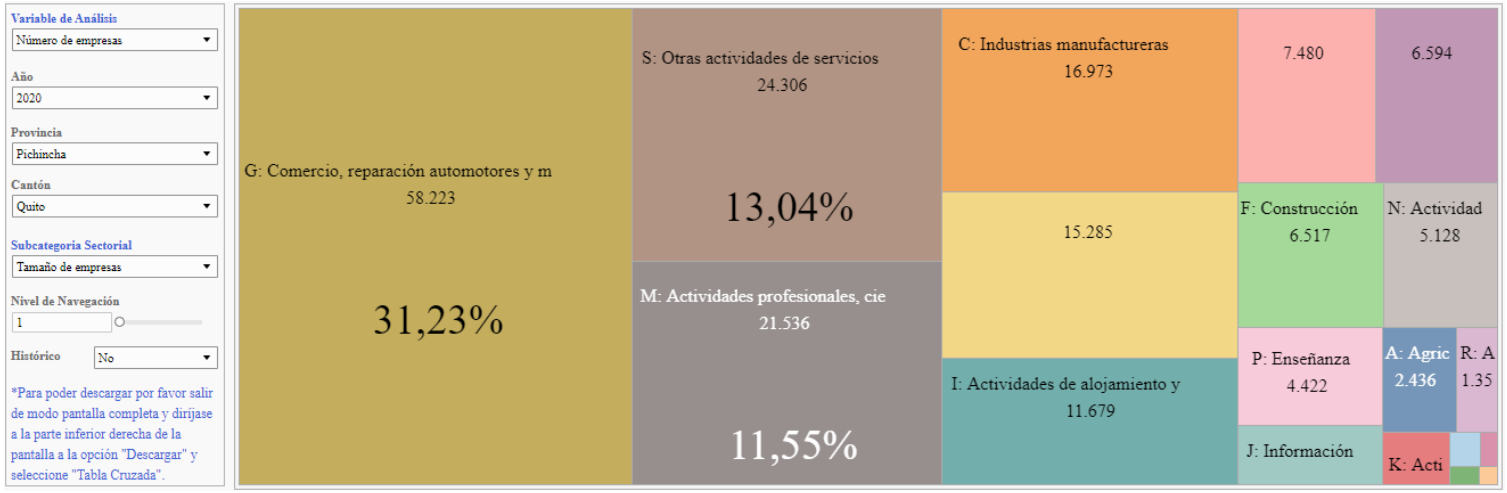
Independientemente del tamaño de la empresa, la correcta implementación de las herramientas de seguridad es fundamental para administrar y mantener adecuadamente una red doméstica, porque hoy en día todo gira en torno a Internet y nunca deja de funcionar, ahora libre de ataques. (robo de contraseñas, robo de identidad, etc.)

Con los datos recabados, se logra develar que existe una brecha significativa de seguridad en las redes usadas por las Microempresas, siendo esta una vulnerabilidad que se ha evidenciado y que requiere una intervención la cual ofrezca una solución a través de la implementación de una herramienta de seguridad de detección de amenazas como es SURICATA.

Idea a defender

Mediante la presente investigación se determinará los diferentes ataques que pueden tener una red de datos tomando en cuenta que en la actualidad la Ciberseguridad es muy preocupante en la mayoría de las Microempresas, ya que según los datos de INEC del 90,3% a nivel Quito el 31,32% pertenece al comercio.

Figura 1:
Estructura sectorial de Número de empresas, subcategoría Tamaño de empresas.



Fuente: (INEC, 2022)

Entonces se pretende saber cuál es la forma más idónea para disminuir los ataques y así tener la información en un resguardo más fiable, tomando en cuenta que existen empresas que manejan datos delicados y pueden llegar a perderse dado que no se aplican estas técnicas adecuadas.

Objetivo de estudio y campo de acción

Objeto de estudio:

En la actualidad existen muchas formas de vulnerar una red, dentro de los cuales se analizará los ataques de análisis de red, ataque de fuerza bruta, phishing. Por tal motivo esta investigación se llevará a cabo dentro de las redes de las Microempresas, para ayudarlas a mantener una mejor protección dentro de las mismas.

Campo de acción:

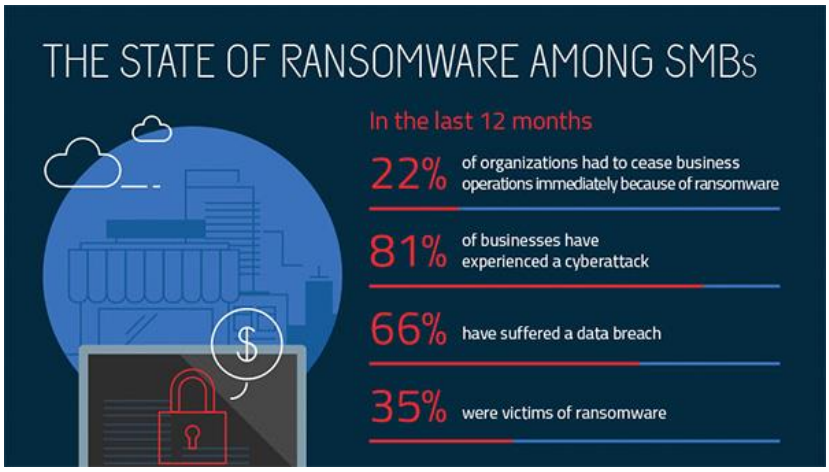
Esta investigación se procederá a realizar dentro de la Micro Empresa T&M Technology, con los dispositivos que estén conectados dentro de la red, por lo cual esto se llevará a cabo con el dispositivo portátil y móvil que son propiedad del investigador, aplicando dicha seguridad para comprobar su eficiencia en la detección temprana en tiempo real de intrusos.

Justificación

Demostrar la existencia de vulnerabilidad dentro de Microempresas, las cuales pueden perjudicar y comprometer a los dispositivos informáticos y a la información existente dentro de los mismos, viéndose afectada debido a ataques cibernéticos tales como: Phishing y Spear Phishing, Spyware, Spoofing, entre otros.

Según informes de Malwarebytes, A fines de 2016, el ransomware representaba el 12,3 % de la investigación de mercado global y solo el 1,8 % de la investigación de consumo global. En 2017, el 35 % de las pequeñas empresas estuvieron expuestas a ataques de ransomware.(Malwarebytes, 2019) Figura 2.

Figura 2:
Informe sobre el ransomware en pequeñas y medianas empresas.



*N*ota: Este informe, fue realizado por Osterman Research y patrocinado por Malwarebytes[3].
Fuente: ***(Malwarebytes, 2019)***

Objetivos

General

- Demostrar que la implementación de una herramienta de seguridad SURICATA puede minimizar las vulnerabilidades de la exigüidad de la seguridad en la red usada por las Microempresas, a fin de lograr la seguridad y confianza de las mismas.

Específicos

- Comprender los conceptos fundamentales de ciberseguridad, las leyes aplicadas en Ecuador y los antecedentes históricos relacionados al proyecto para implementar un tema de manera adecuada y efectiva.

[3] Presenta los hallazgos sobre ransomware y otros críticos problemas de seguridad de más de 1.000 pequeñas y medianas organizaciones encuestadas en junio de 2017. Tomado de https://www.malwarebytes.com/pdf/infographics/malwarebytes_the_state_of_ransomware_among_smbs.pdf

- Analizar las cifras de concientización de las personas encargadas en las empresas y sus vulnerabilidades para determinar los resultados estadísticos y analíticos del proyecto.
- Cubrir la parte práctica del proyecto, específicamente en la configuración de la herramienta de seguridad, a través de la utilización de ataques en Kali Linux y la configuración de IDS e IPS para proteger los sitios web específicos.
- Determinar y analizar el trabajo de desarrollo y los costos asociados a cada fase del proyecto real.

Síntesis de la introducción

En la década de 1970, la seguridad corporativa se centró en garantizar que los empleados usaran la información necesaria, confiando en el sentido común para mantener segura a la organización. Sin embargo, con la inclusión y el avance de la tecnología han surgido nuevos riesgos que inutilizan la "seguridad".(INCIBE, 2015).

Muchas empresas no le dan la importancia suficiente a la seguridad informática, lo que puede causar problemas en cuanto a vulnerabilidades y configuraciones inadecuadas. Sin embargo, existen herramientas que pueden ayudar a monitorear y analizar estos problemas, brindando soporte adicional a los departamentos de TIC. Es importante tener en cuenta que la información proporcionada por estas herramientas puede ser difícil de entender, y se recomienda el uso de herramientas como SURICATA, que son fáciles de usar y comprender.

CAPÍTULO I: FUNDAMENTACIÓN TEÓRICA

Antecedentes históricos

El ciberespacio ha intercalado una nueva dimensión en la sociedad de una forma cotidiana y generalizada, de tal manera que gracias a estas nuevas tecnologías y su uso dentro del Internet. Todos estos aspectos de un uso y una estadía dentro del ciberespacio conllevan a una dependencia del mismo ya que todas las cosas que hacemos en la actualidad se basan en su uso, ya sea por hobbies o por trabajo se usa el internet para navegar en las redes sociales y son estas últimas las que en la actualidad son parte del trabajo de las empresas y emprendedores debido a que por medio de las redes sociales promocionan sus productos.

Los emprendedores, pequeñas empresas y microempresas tienen como objetivo primordial promocionar sus negocios y sus productos realizando marketing a través del Internet, para lograr así sus metas, lamentablemente no toman en consideración el riesgo que esto implica al no disponer de una adecuada seguridad al utilizar este servicio, debido a esto sobrelleva una carga ocasionando muchas brechas de seguridad que afecta a su empresa.

Este hecho de no poseer un conocimiento y concientización adecuada de navegación y conexión segura les convierte en agentes vulnerables para los Crackers ya que estos les visualizan como potenciales objetivos bien sea para realizar prácticas o para hacer ataques de phishing mediante los cuales llegan a empresas más grandes o directamente a sus proveedores. Este grupo piensa que los proveedores de internet (ISP), son los encargados de brindar ese soporte de una conexión segura a internet.

Cada vez que una brecha en la seguridad de una empresa se ve afectada o golpeada es ahí cuando empiezan a tomar en serio las medidas de seguridad, intentan ver a la ciberseguridad como una inversión más no como un gasto, como normalmente suele ser. “Muchas organizaciones pequeñas prestan poca atención a la ciberseguridad o la seguridad de la información y, a menudo, fallan debido a su incapacidad para prevenir, prevenir o gestionar ataques.”(Solutions, 2019).

Sin embargo, como se había mencionado anteriormente estos son errores que pueden ser mitigados, pero debido al hecho de que no se tiene una concientización de protección cibernética, estos errores simples son omitidos por las Microempresas, a continuación, se detallará de manera efímera las claves que no se deben pasar por alto para evitar estos problemas:

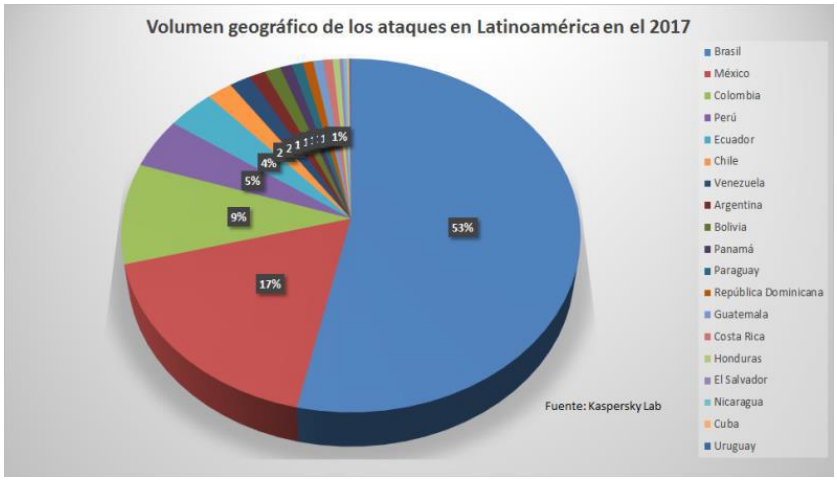
- Sin política de privacidad.
- Falta de formación en sensibilización del personal.
- Evitar copias de seguridad.
- Acceso desatendido a la infraestructura.
- No tener copias en la nube.
- No realizar actualizaciones.
- Financiación insuficiente para asegurar datos.
- Contraseñas mal manejadas.
- No existe un proceso para despedir empleados.
- Fiándose en productos de grado de consumo.

La BBC publicó un informe que indica que en septiembre de 2016 hubo un promedio de 12 ataques informáticos por segundo en América Latina y

Centroamérica. Según esta información, Ecuador ocupa el octavo lugar con un 36,1% de ataques dirigidos a usuarios conectados.

Según datos de Kaspersky Lab, en septiembre de 2017, la misma región experimentó un promedio de 33 ataques por segundo, ubicando a Ecuador en el quinto lugar en cuanto a número de ataques, como se muestra en la Figura 3.

Figura 3:
Países de Latinoamérica vs ataques informáticos.



Fuente: (LARA GUIJARRO, 2019, pp. 14, 18)

Tanto en el Ecuador como en el mundo, debido al desarrollo de la tecnología, los problemas en las redes de información son motivo de gran preocupación ya que se relacionan con la tasa de piratería o alteración de la información. La vulnerabilidad de los sistemas ante posibles ataques es un factor que afecta la integridad y seguridad de los datos en diferentes organizaciones.(LARA GUIJARRO, 2019, pp. 14, 18)

La mayoría de las Microempresas usan el servicio prestado por el ISP, el mismo que lo emplean para realizar actividades tanto de trabajo como personal, las cuales tienen conexión inalámbrica lo que presenta una vulneración aún mayor ya que no constan con una seguridad especializada para tener una respuesta ante incidentes, los cuales pueden ser no solo la vulneración de la red sino la perdida, captura y difamación de los datos que se manejan en dichas empresas.

El ciberespacio es un ambiente complejo resultante de las interacciones de la gente, software y los servicios en el internet que se sustentan en los apartados físicos y las redes interconectadas de tecnología de la información y de comunicaciones, esto aplica tanto para proveedores de servicio como para consumidores que utilizan esos servicios. Dentro de la ISO/IEC 27032:2012, uno de los puntos primordiales de esta norma es el enfoque de la seguridad del Ciberespacio (Ciberseguridad) ante ataques tales como:

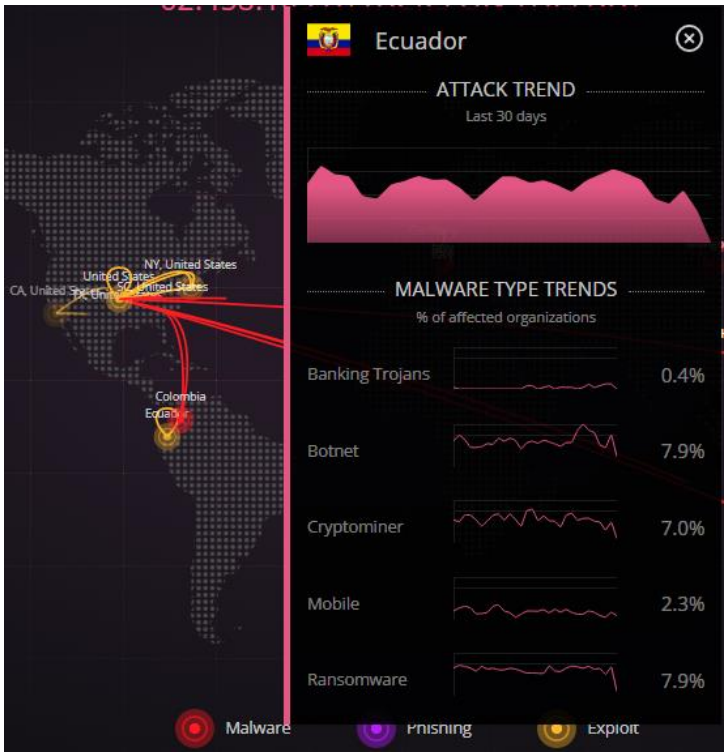
- Ataques de Ingeniería Social.
- Proliferación de Malwares y Spywares.
- El acceso no autorizado a sistemas informáticos.
- Respuesta ante amenazas.
- Detección y monitoreo de ataques.

Según el Reporte de Ciberseguridad 2020 “Riesgos, Avances y Perspectivas en América Latina y el Caribe” y “Modelo de Madurez de Competencias en Ciberseguridad”, Ecuador no cuenta con una estrategia de ciberseguridad a pesar de que se han logrado avances significativos en materia de seguridad de redes. Guardia. Desde 2018, el BID brinda asesoría técnica al país para mejorar la gestión de los equipos de inteligencia de amenazas, aunque el sector privado brinda asistencia urgente, según un estudio de Deloitte, en 2018 mostró que el 50% de las empresas han implementado un programa de concientización sobre ciberseguridad para empleados. Sin embargo, el 70% de las organizaciones dijeron que no estaban seguros de la efectividad del proceso de respuesta a incidentes de ciberseguridad.”(OEA; BID, 2020, p. 93). No obstante, el País en la actualidad enfrenta un gran déficit de profesionales de seguridad cibernética, a pesar de que

las universidades privadas y públicas ofrezcan cursos enfocados en seguridad cibernética.

Según la gráfica de estadística en tiempo real de la empresa Check Point, sobre los ataques más recurrentes dentro de los últimos 30 días se visualiza, como el Ecuador ha sido víctima como top tres de: Ransomware, Botnets y Criptominería.

Figura 4:
Mapa en tiempo real de ataques cibernéticos.

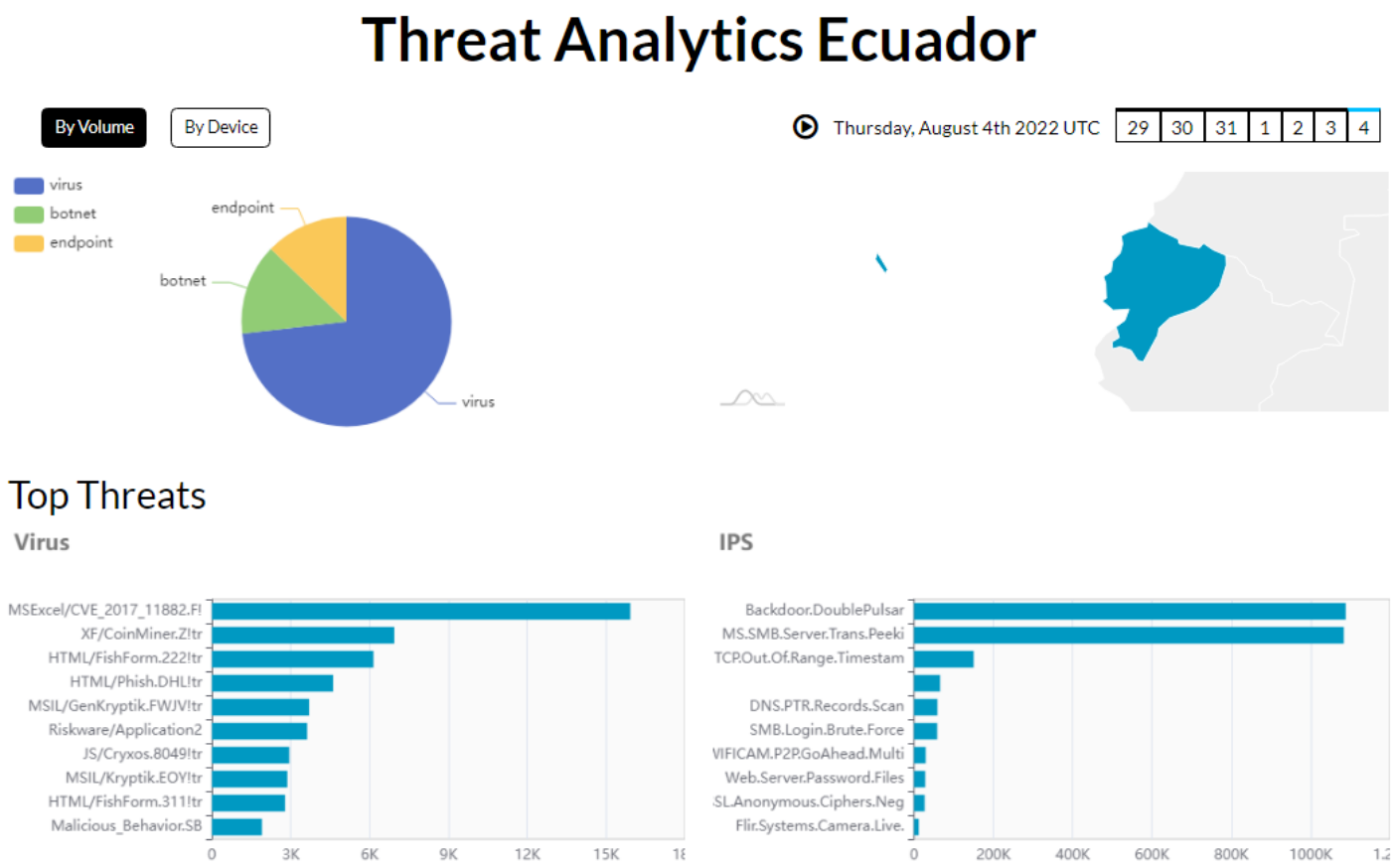


Fuente: (Check Point ThreatCloud, 2022)

Acorde a las estadísticas por parte de la empresa FORTINET, especialista en Seguridad cibernética muestra a la fecha de la consulta (04/08/2022) de igual forma un top de amenazas recurrentes en el País, siendo estas estadísticas de dos formas por volumen y por equipo.

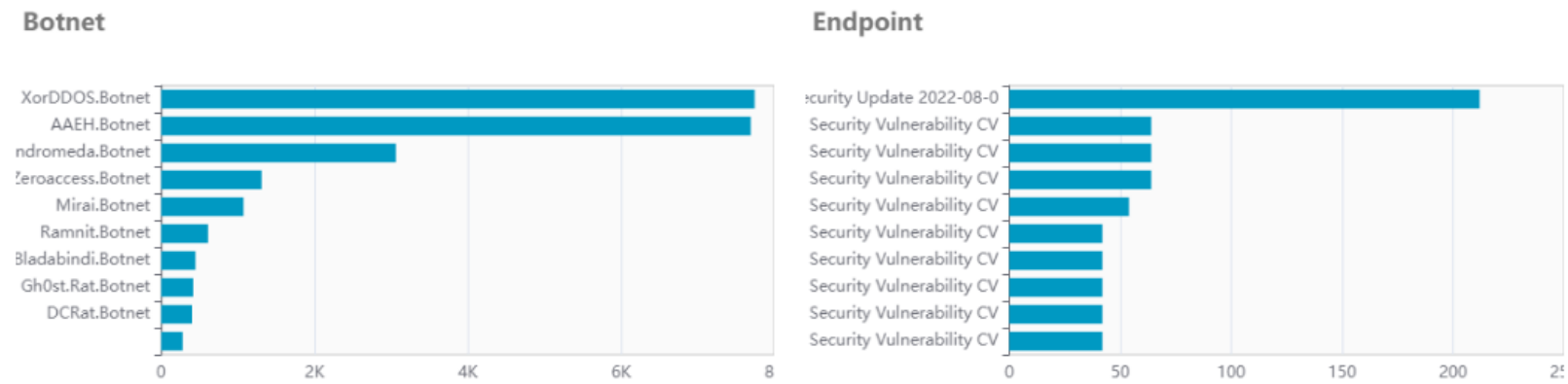
- Por Volumen

Figura 5:
Estadísticas del top de amenazas más frecuentes en el Ecuador por volumen.



Fuente: (FortiGuard, 2022)

Figura 5.1:
Estadísticas del top de amenazas más frecuentes en el Ecuador por volumen.

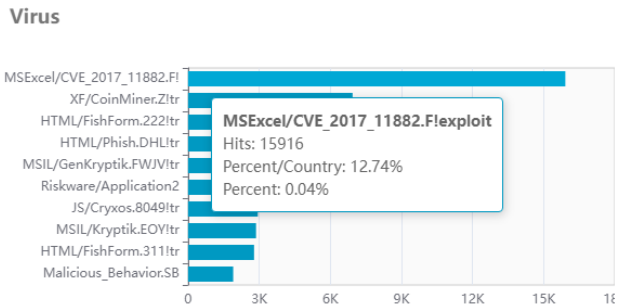


Fuente: (FortiGuard, 2022)

Los dos casos más preocupantes que existen actualmente son violaciones por falta de actualizaciones de programas periodicamente porque la licencia original no esta disponible o las actualizaciones automáticas estan desactivadas. En estos dos ejemplos que se muestran a continuación, se identifica una brecha de seguridad en Microsoft Excel (CVE_2017_11882.Flexpoint). Acorde al informe presentado por la propia compañía (Microsoft Security Response Center), informan que “esta es una vulnerabilidad de daños en la memoria de Microsoft Office, una vulnerabilidad de ejecución remota de código en el programa de Microsoft Office ocurre cuando el software maneja incorrectamente los objetos en la memoria.”(Microsoft MSRC, 2017).

Siendo que esta vulnerabilidad ya ha sido parchada para versiones posteriores a las del 2017, aún siguen existiendo y encabezando la lista de las vulnerabilidades en el País, esto se debe a la fata de actualizaciones o al uso no apropiado de una licencia dentro de las empresas y hogares del Ecuador.

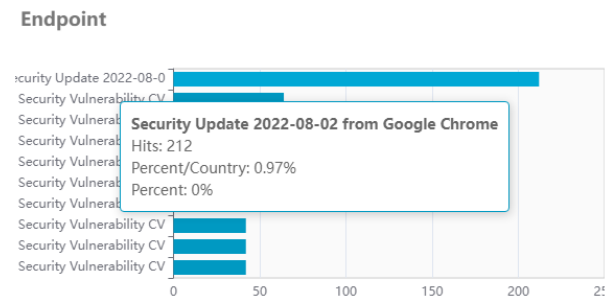
Figura 6:
Exploit: Win32/CVE-2017-11882.



Fuente: (FortiGuard, 2022)

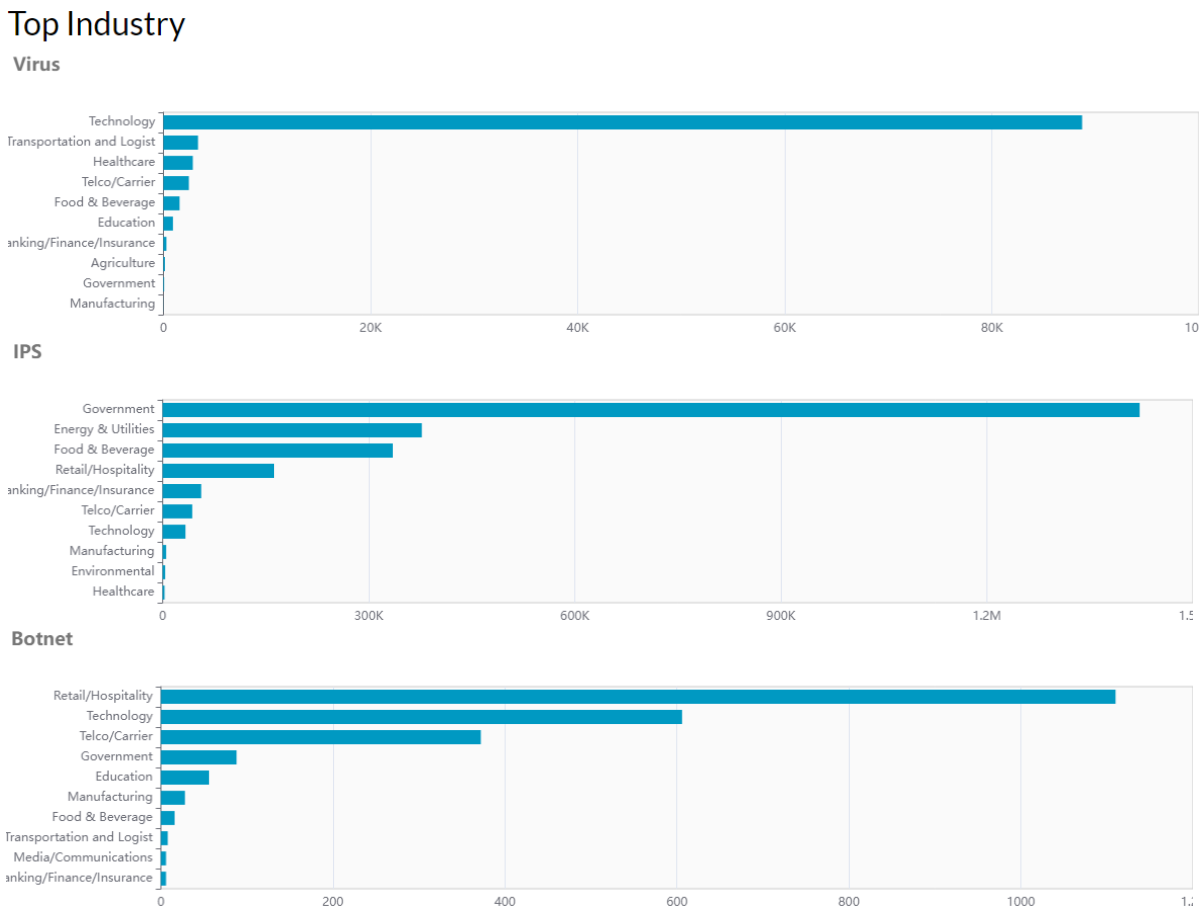
De igual manera en los dispositivos finales se tiene una gran brecha de seguridad por motivos de no actualizar los navegadores basados en Chromium, este sistema operativo es especialmente diseñado para los Navegadores, estas grietas pueden causar grandes perdidas de datos debido a toda la información que se maneja dentro de los nevegadores, como son las credenciales de accesos a redes sociales, cuentas bancarias y un sin número de datos que se digita e ingresa diariamente ya sean por compras, trabajo o desenvolmimiento personal.

Figura 7:
Actualización de firmware 2022-08-02 Google Chrome.



Fuente: (FortiGuard, 2022)

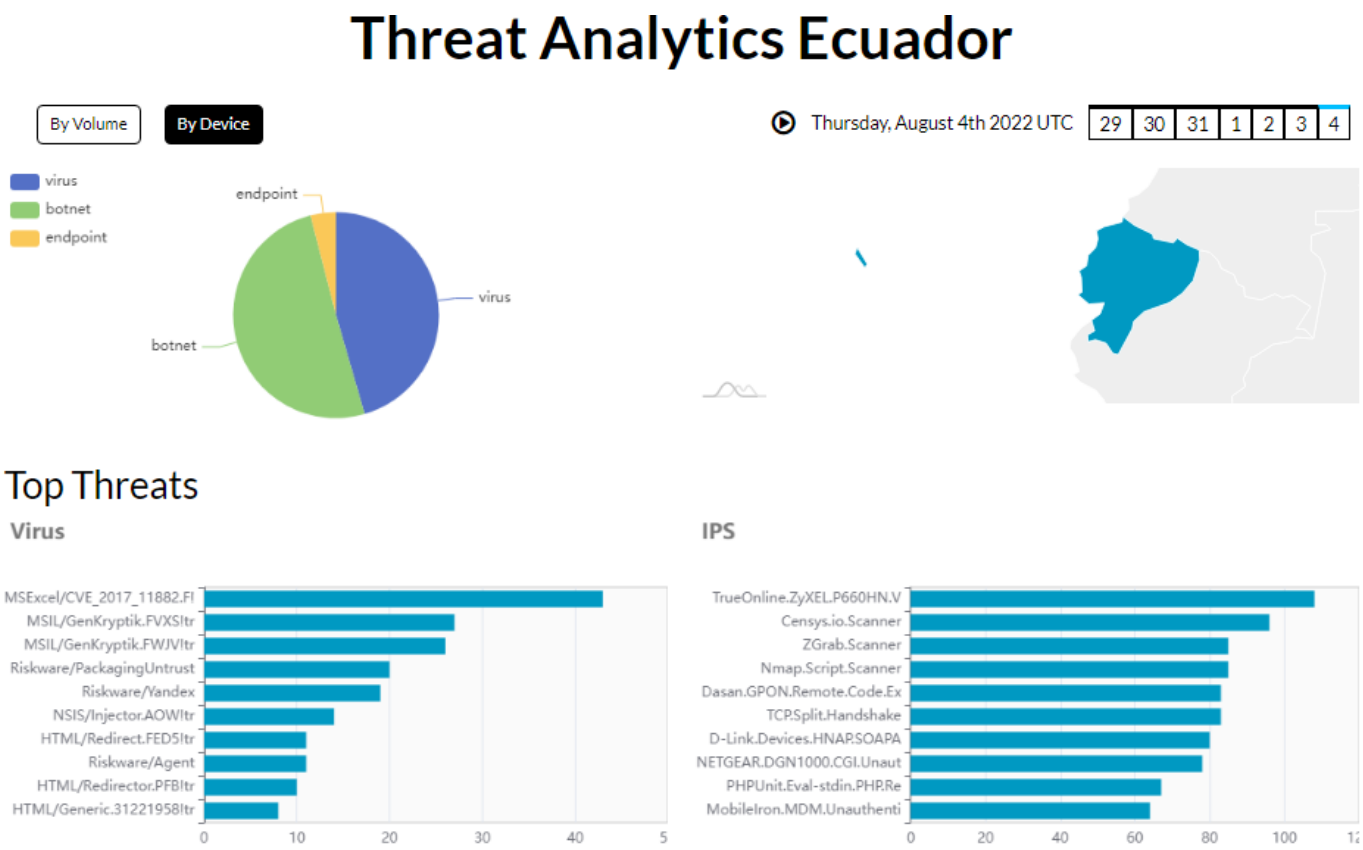
Figura 8:
Top tipo de industrias más afectadas.



Fuente: (FortiGuard, 2022)

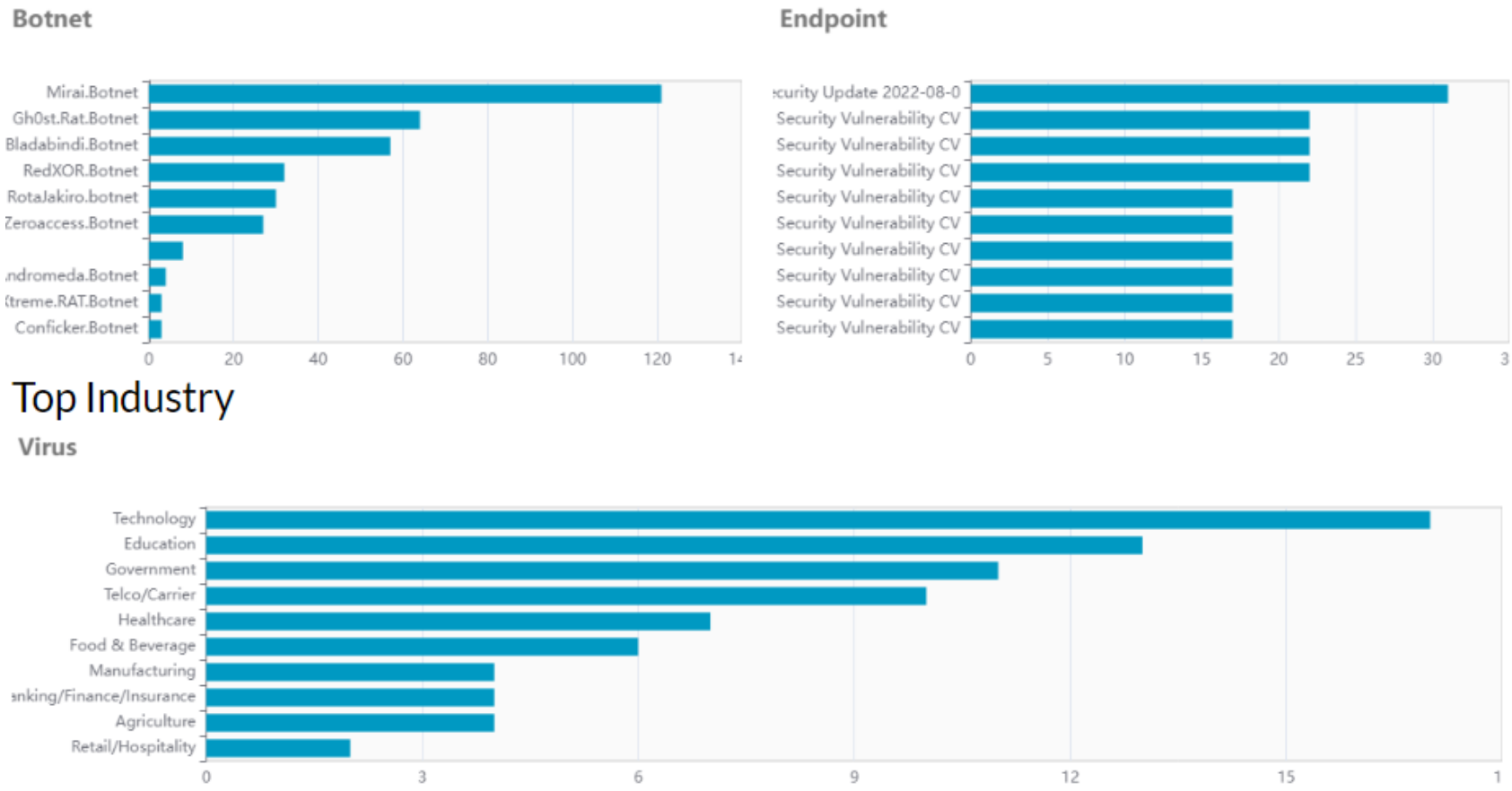
- Por Equipo

Figura 9:
Estadísticas del top de amenazas más frecuentes en el Ecuador por equipo.



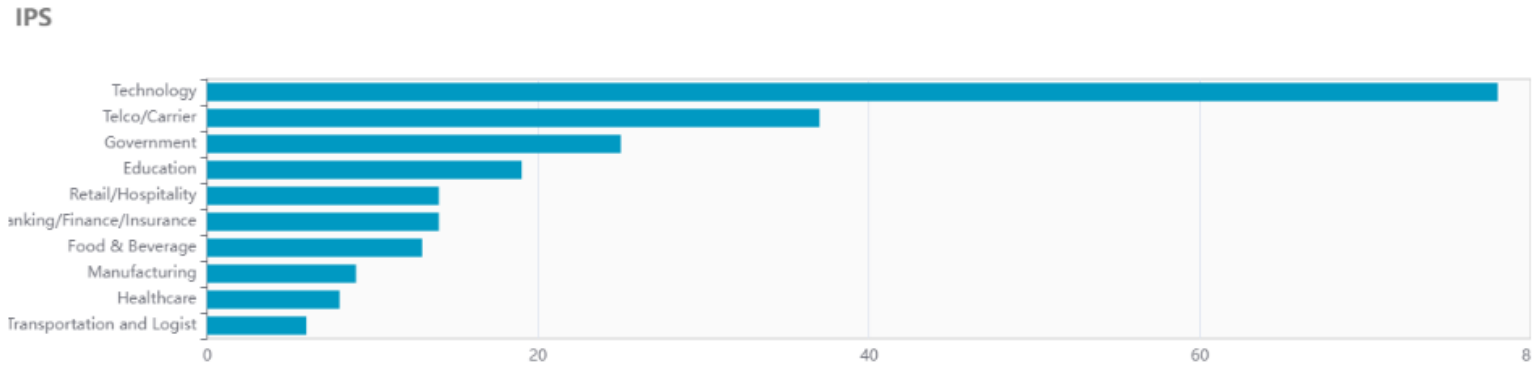
Fuente: (FortiGuard, 2022)

Figura 9.1:
Estadísticas del top de amenazas más frecuentes en el Ecuador por equipo.



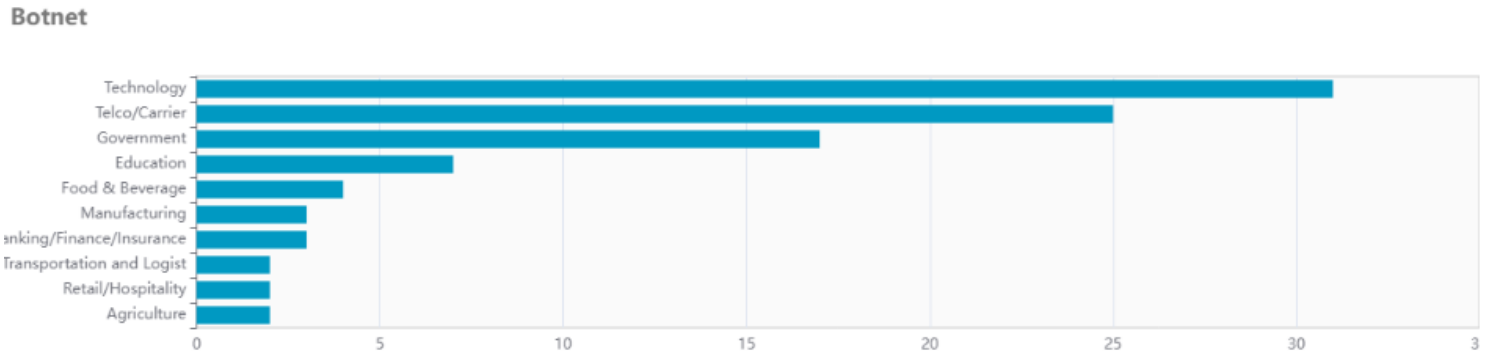
Fuente: (FortiGuard, 2022)

Figura 9.2:
Estadísticas del top de amenazas más frecuentes en el Ecuador por equipo.



Fuente: (FortiGuard, 2022)

Figura 9.3:
Estadísticas del top de amenazas más frecuentes en el Ecuador por equipo.



Fuente: (FortiGuard, 2022)

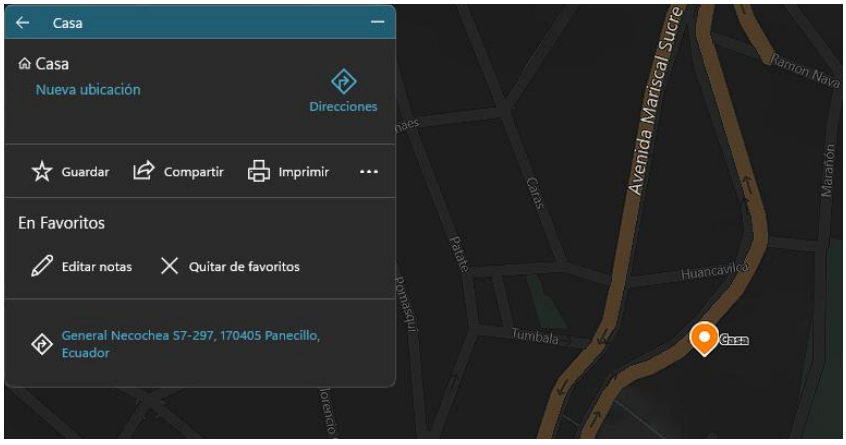
En el muestreo se evidencia información de las vulnerabilidades las cuales han sido explotas por medio de las APT (Advanced Persistent Threat) por sus siglas en ingles de Amenaza Avanzada Persistente las mismas que se rigen a la Matriz Mitre ATT&CK.

Todas las empresas después de verse afectadas buscan una solución, sin pensar que todas las pérdidas y daños, se pueden evitar teniendo la ayuda de una sola herramienta que es SURICATA; la cual permite tener un control adecuado de la red.

Por lo expuesto, el presente proyecto pretende demostrar las falencias y las carencias que mantienen las redes domesticas al momento de ser usadas para realizar el trabajo y tener un uso personal al mismo tiempo, sin tener una segmentación o una herramienta de contención y respuesta ante ataques realizados a las redes Wi-Fi.

Análisis de la zona de estudio

Figura 10:
Ubicación empresa T&M Technology.



Fuente: (Mejía, 2022b)

Nota: La imagen corresponde a la ubicación de la microempresa T&M Technology, sacada de Mapas Microsoft Corporation.

La casa donde se encuentra ubicada la microempresa T&M Technology tiene una superficie total 1.800 m^2, cuenta con dos departamentos centrales, en uno de ellos se encuentra la residencia y la oficina, la cual consta de un piso distribuido con dos habitaciones y una oficina.

Fundamentación Conceptual

Los Crackers son individuos maliciosos que intentan acceder a los sistemas informáticos sin autorización. (Network Working Group, 1993, p. 12)

Un hacker es alguien que tiene un amplio conocimiento del funcionamiento interno de los sistemas informáticos, dispositivos y redes. El término se usa incorrectamente en un contexto peyorativo donde Cracker sería el término correcto. (Network Working Group, 1993, p. 21)

Un IDS o Sistema de Detección de Intrusos, sirve para detectar accesos no autorizados a una red o aun ordenador, permitiendo monitorizar el tráfico entrante ante cualquier actividad sospechosa emitiendo una alerta. (INCIBE, 2020)

IPS o Intrusion Prevention System, como su nombre indica, se utiliza para proteger de forma proactiva el sistema contra ataques e intrusiones al permitirle controlar el acceso a la red de la misma manera que se basa en el control. (INCIBE, 2020)

Network Security Monitoring (NSM) recopila y analiza datos, lo que a su vez brinda a las empresas la capacidad de detectar y responder a los intrusos que ingresan a sus redes. (Güelfo, 2016)

La captura de paquetes o PCAP (también conocida como libpcap) es una interfaz de programación de aplicaciones (API) que captura datos de paquetes de red en vivo de las capas 2-7 del modelo OSI.(Torres, 2021)

Amenaza persistente avanzada (APT) es un término amplio utilizado para describir una campaña de ataque en la que un atacante o grupo de atacantes establece una presencia de phishing a largo plazo en la red para extraer datos altamente confidenciales. (Shabi et al., 2019)

MITRE ATT & CK son las siglas de MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT & CK). La plataforma MITRE ATT&CK es una base de conocimientos y un modelo de comportamiento ciberdelincuente cuidadosamente construidos que refleja las diferentes etapas en el ciclo de vida del atacante y la plataforma identificada como objetivo. (Ciberseg1922, 2021)

Las Microempresas son un grupo de empresas a las cuales pertenecen Micro, medianas y pequeñas empresas con un número reducido de empleados y un nivel de liquidación moderado que representan en la mayoría de los países el motor de la economía. (Logística Actualizada, 2014)

Fundamentación Legal

- Acorde a la Resolución AG/RES 2004 (XXXIV-O / 04) de la Organización de Estados Americanos (OEA), se resuelve en el literal dos y seis “Instar a los Estados Miembros y a los órganos, organismos y entidades de la OEA a que coordinen sus esfuerzos para incrementar la seguridad cibernética e implementar dicha estrategia.”(Cuarta sesión plenaria OEA, 2004).
- De igual forma en el Código Orgánico Integral Penal (COIP) en los Art. 178, Art. 190, Art. 233 y Art. 234. Nos indica que aquella persona sin algún consentimiento o autorización legal, comparta, divulgue o difunda datos personales de otra persona sea por apropiación fraudulenta mediante la

manipulación y vulneración, del funcionamiento de equipos terminales de telecomunicaciones, programas, redes electrónicas, el acceso logrado, modificación de un portal web o redireccionamiento del tráfico de datos en beneficio suyo utilizando dichos métodos, será sancionada con pena privativa de libertad de uno a tres años y en el caso de los Art. 233 y Art. 234 serán sancionados con la pena privativa de la libertad de tres a cinco años. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2021)

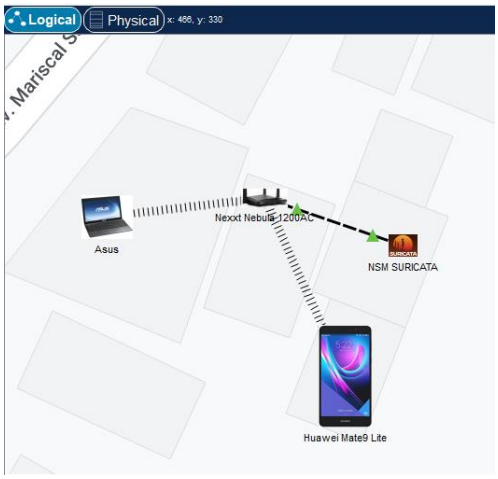
- De acuerdo con la ley orgánica de telecomunicaciones, art. 76, enfatiza que los proveedores de servicios, ya sean redes propias o de terceros, deben tomar medidas técnicas y de gestión para garantizar la seguridad del servicio y la impenetrabilidad de las brechas de la red, para mantener y garantizar la protección de las comunicaciones y la información misma. transmite a través de sus redes, asegurando un nivel adecuado de seguridad frente a amenazas.(LEY ORGÁNICA DE TELECOMUNICACIONES, 2015, p.22)
- En la Resolución Arcotel-2018-0652 expón “que en el capítulo II del Título VII de la LOT, se establece la protección de Datos Personales, constatando, entre otros, los siguientes artículos:”(ARCOTEL, 2018, pp. 2-3).
    - Art. 78. Para la validez del derecho de la intimidad establecido en el Art. 66, numeral 20 de la Constitución de la República del Ecuador, los prestadores de servicios de telecomunicaciones deberán garantizar la protección de los datos de índole personal, para dicho efecto deberán optar por medidas técnicas y de gestión para preservar la seguridad de la su red.

- Art.84. Los prestadores de servicios, emitirán a las autoridades rectoras la información que requerían dentro de un proceso legal ante una investigación de delitos, siendo la ARCOTEL quien instituya los mecanismos y ordenamientos que sean precisos.
- Art. 85. la ARCOTEL instituirá y normalizará los mecanismos para supervisar el cumplimiento de las obligaciones de seguridad de datos personales que serán vinculantes para los prestadores de servicios con el fin de salvaguarden las medidas relativas a la integridad y seguridad de las redes y servicios.

Todo esto se visualiza de manera más resumida dentro del Acuerdo Ministerial 006-2021 Política de Ciberseguridad del Ministerio De Telecomunicaciones Y De La Sociedad De La Información.

Fundamentación Técnica y/o Tecnológica

Figura 11:
Topología de la red con Suricata.



Fuente: (Mejía, 2022a)

Suricata

La herramienta de seguridad SURICATA permite tener en un solo programa un Sistema de Detección de Intrusos (IDS); Sistema de Prevención de Intrusos (IPS); Monitoreo de Seguridad de Red (NSM) y Procesamiento (PCAP), los cuales nos dan un monitoreo en tiempo real de todas las inconsistencias o amenazas que se puede presentar dentro de la red local.

La implementación de la herramienta en una topología MyPimes se realiza mediante un servidor (virtual o físico) con Windows o Linux, lo cual permite la versatilidad y la simplicidad en el manejo de esta herramienta.

Síntesis del capítulo

En el presente capitulo se toma en cuenta la parte teórica del proyecto y la importancia que va a dar cada uno de ellos al momento de realizar o implementar mi tema realizado, haciendo énfasis en los conceptos de ciberseguridad, leyes aplicadas en Ecuador y los antecedentes históricos.

CAPÍTULO II: DIAGNÓSTICO

Tipos de investigación

- **EXPLORATIVA:** Según Enrique Rus "Así, la investigación exploratoria se ocupa de un tema que no ha sido estudiado antes o permite descubrir nuevos aspectos del conocimiento existente. Entonces, cuando no se entiende cual es el problema al que se puede llegar a enfrentar, es mejor hacer una investigación antes de hacer otro análisis más costoso." (Arias, 2022)

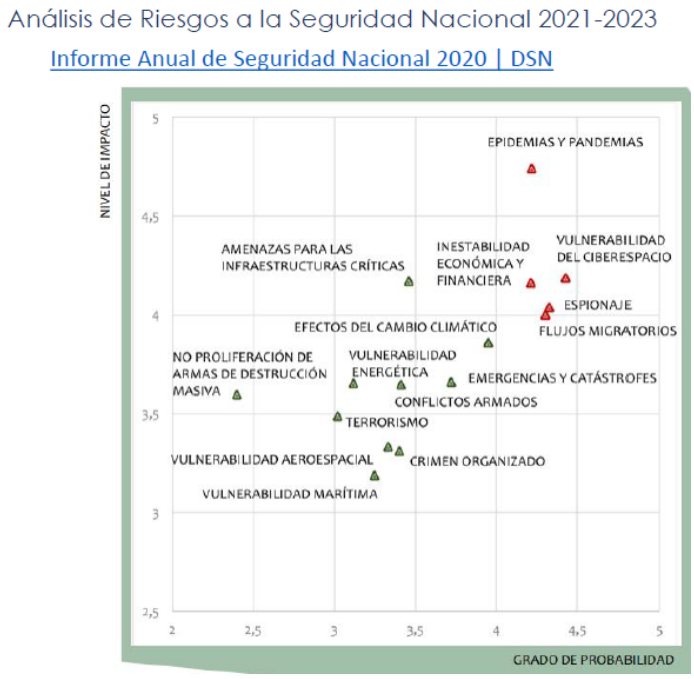
  Esta investigación permite focalizar un tema que es muy controversial, siendo que no solo dentro del país tiene varias brechas si no que a nivel internacional presenta una carencia de seguridades dentro de las Pymes y MiPymes.

Métodos de investigación

- **ANALÍTICO:** Este método permite echar un vistazo a las partes tanto poblacional como empresarial, dejando notar como influye la concientización de las personas dentro y fuera de su ámbito laboral la cual resulta ser las mismas prácticas de seguridad y metodología dentro de internet.

  Como ejemplo se puede manifestar que dentro de las Pymes de España existe margen de riesgo de nivel de impacto y nivel de probabilidad ambos altos (4 en la escala) los hechos como: vulnerabilidad del ciberespacio.

Figura 12:
Análisis de Riesgos a la Seguridad Nacional 2021-2023.



Fuente: (*Informe Anual de Seguridad Nacional 2020 | DSN*, 2021)

En la contra parte ecuatoriana existe un porcentaje del 75% que no saben y no son conscientes de las acciones realizadas e impacto que tienen en internet. Lo cual es muy crítico tanto para la seguridad e integridad empresarial como personal, esta criticidad se debe a la desinformación que se presenta en la actualidad dentro de la sociedad, en la antigüedad se pecaba por no tener información a la mano; ahora en la actualidad se tiene un acceso excesivo a la información y este es uno de los motivos por los cuales las poblaciones no saben que es verdad y que es falso o simplemente no es de su interés.

Técnicas e instrumentos de investigación

- **ENTREVISTA:** Dialogo entre dos personas, de manera virtual organizada por mí persona. Preguntas a realizar

1. **¿Usted es el encargado o director de seguridad en la empresa?**
2. **Usted ha escuchado o leído sobre ¿qué es un soc?**
3. **Usted sabe ¿cuáles son los beneficios que le puede ofrecer un soc?**
4. **¿Qué tipo de ataques conoce usted?**
5. **Ha sufrido algún tipo de vulneración, ¿qué tipo de vulneración fue?, en el último año (malware, hackeo, phishing)**
6. **¿Qué medidas de seguridad tomó para contenerla?**
7. **¿Conoce usted los sistemas de seguridad de red como: ids, ips, siem, ossec?**
8. **Tiene implementado en la red algún sistema de seguridad. ¿cuál?**
9. **¿Estaría dispuesto a realizar una migración o implementación de un sistema de seguridad tipo soc para su empresa? Si, no, por qué.**
10. **En el caso de que la empresa, no esté preparada para un ataque cibernético. ¿usted estaría dispuesto a pagar el rescate de la información?, ¿cuánto estaría a pagar?**

- **ENCUESTA:** Registro de respuestas con ayuda de un cuestionario. Tipo de encuesta y Modelo de encuesta a ejecutar (luego lo coloca al final del trabajo)

Universo y muestra

Universo:

- En el cantón Quito actualmente se encuentran 186.445 empresas de acuerdo a las estadísticas del INEC realizadas en el 2020.

Muestra:

Tipo. - Probabilística

- En el cantón Quito actualmente se encuentran 186.445 empresas de acuerdo a las estadísticas del INEC realizadas a la fecha actual del 2020. La investigación se enfocará al segmento "Financiera y de seguros" en la cual existe 1.083 empresas que representa al 0,58% del total de empresas a nivel Quito.

Figura 13:
Estructura sectorial de número de empresas, subcategoría, tamaño de empresas.

Fuente: (INEC, 2022a)

El segmento financiero y de seguros es uno de los más activos y que consta con información sensible de los usuarios, ya sean estos particulares o empresas tales como: la cantidad de bienes, números de activos, números de cuentas, nombres datos personales como: Cédula de identidad, correo electrónico, número celular, dirección domiciliaria.

Fórmula establecida

Aunque existe varias formas de encontrar la muestra para poblaciones finitas, la fórmula a utilizar es:

$$n = \frac{z2 * p * q * N}{(N * e2) + (z2 * p * q)}$$

Donde:

n= Tamaño de nuestra muestra

Z= Nivel de confianza = 95% = 1,96

N= Población de estudio

e= Error de estimación = 0.05

p= Probabilidad de éxito = 0.5

q= Probabilidad de fracaso = 0.5

$$n = \frac{1{,}96(2) * \ 0.5 * 0.5 * 1.083}{(1.083 * 0.05(2)) + (1{,}96(2) * 0.5 * 0.5)}$$

$$n = \frac{3{,}84 * \ 0.5 * 0.5 * 1.083}{(1.083 * 0{,}0025) + (3{,}84 * 0.5 * 0.5)}$$

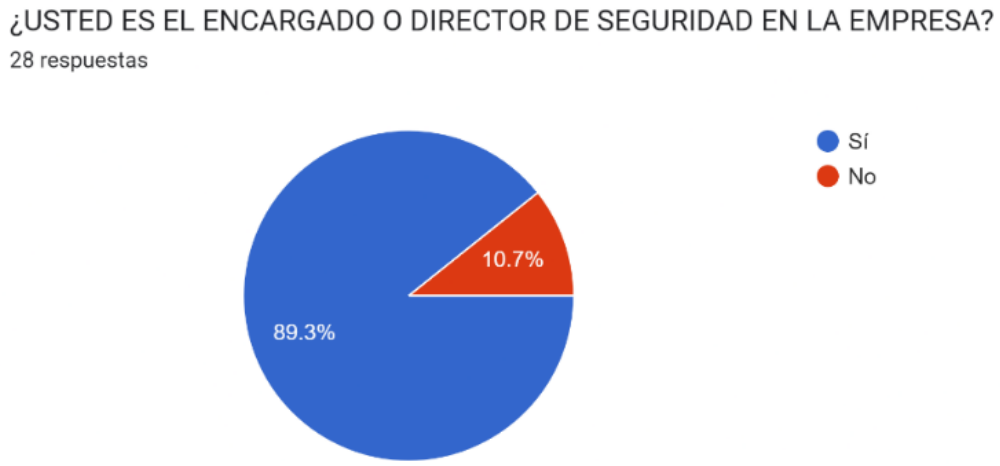
$$n = \frac{1.039{,}68}{2{,}7075 + 0{,}96}$$

$$n = \frac{1.039{,}68}{3{,}6675}$$

$$n = 283$$

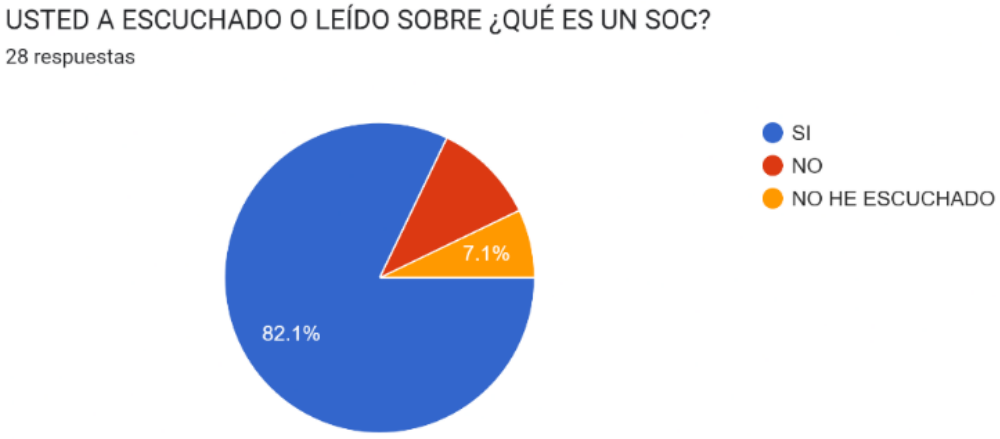
Presentación gráfica, análisis e interpretación de resultados obtenidos

Figura 14:
Encuesta Pregunta 1.



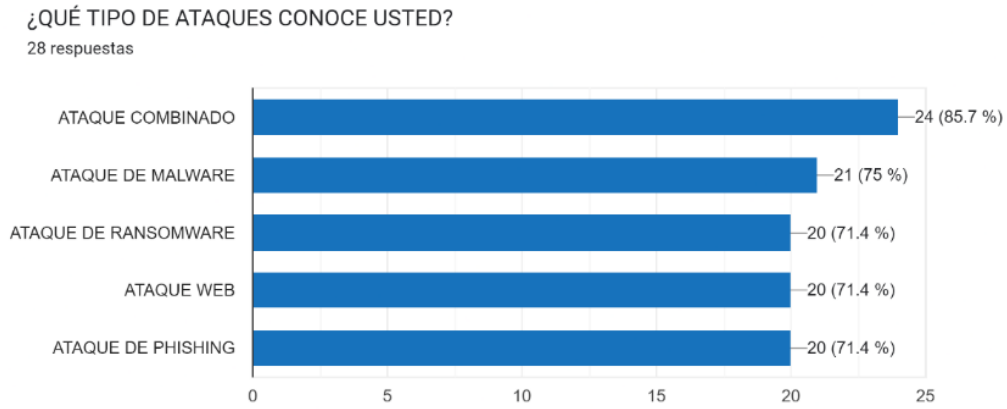
***Nota**: El gráfico muestra por porcentajes las diferentes opciones de respuesta de la Pregunta 1*

Figura 15:
Encuesta Pregunta 2.



Nota: El gráfico muestra por porcentajes las diferentes opciones de respuesta de la Pregunta 2

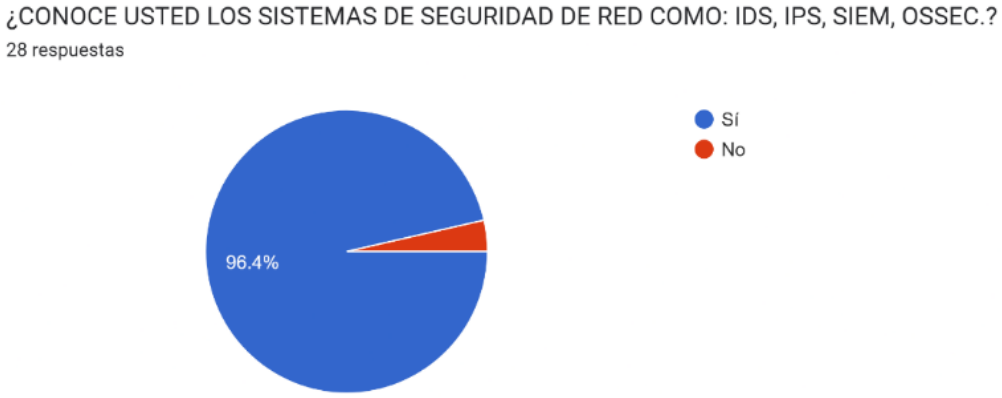
Figura 16:
Encuesta Pregunta 4.



Nota: El gráfico muestra por porcentajes las diferentes opciones de respuesta de la Pregunta 4.

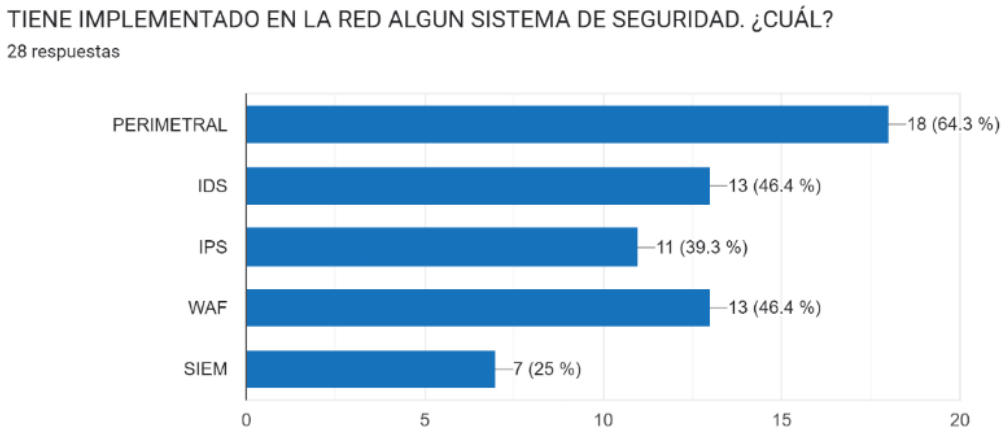
Figura 17:

Encuesta Pregunta 7.



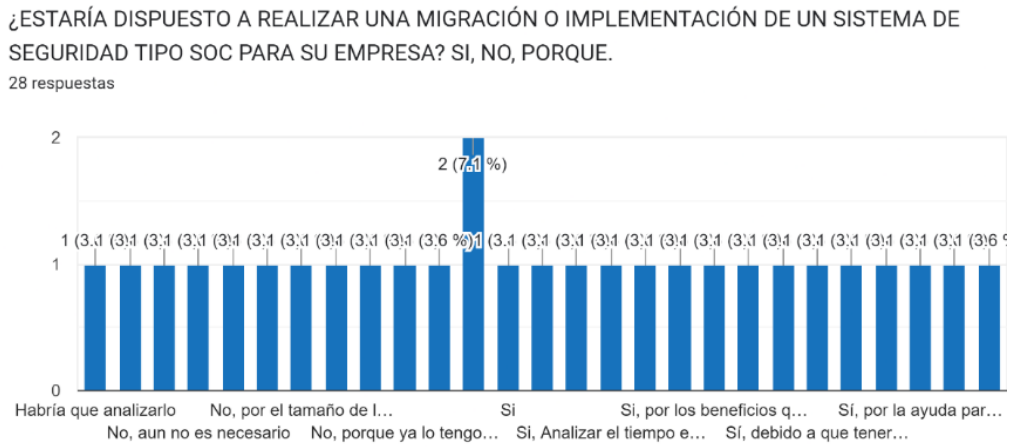
Nota: El gráfico muestra por porcentajes las diferentes opciones de respuesta de la Pregunta 7

Figura 18:
Encuesta Pregunta 8.



Nota: El gráfico muestra por porcentajes las diferentes opciones de respuesta de la Pregunta 8.

Figura 19:
Encuesta Pregunta 9.



Nota: El gráfico muestra por porcentajes las diferentes opciones de respuesta de la Pregunta 9.

Figura 20:
Encuesta Pregunta 10.

Nota: El gráfico muestra por porcentajes las diferentes opciones de respuesta de la Pregunta 10

Análisis e interpretación de resultados

Acorde a las encuestas obtenidas de las 28 empresas se determina que:

- El 96.4% de las empresas encuestadas tienen un conocimiento de los sistemas de seguridad de red.
- El 64.3% de las empresas encuestadas tienen como sistema de protección un software perimetral, el 46.4% de las empresas tienen implementado un IDS y un WAF, el 39.3% de las empresas tienen un IPS dentro de la red para su protección y el 25% tienen implementado un SIEM como herramienta de seguridad dentro de la red de la empresa.
- El 32.14% de las empresas encuestadas, han tomado medidas precautelarías después de haber sufrido un ataque de ingeniería social.
- El 28.6% de las empresas encuestadas no han hecho nada después de recibir un ataque cibernético.

Llegado a un análisis que todas las empresas han sufrido un ataque ya sea por ingeniería social, phishing o de malware, y que han tomado cartas sobre el

asunto acorde al presupuesto que manejan y dando varias capacitaciones al personal no técnico de cómo deben actuar y manejar ante dichos ataques.

Síntesis del capítulo

En el actual capitulo se toma en cuenta la parte estadística y la parte analítica la cual va a dar en cifras los resultados de concientización que tienen las personas encargadas dentro de las empresas y sus vulnerabilidades.

CAPÍTULO III: PROPUESTA

Descripción de la propuesta

Demostrar la importancia que se tiene al momento de tener implementado una herramienta de seguridad dentro de una red de datos como lo es SURICATA, la cual admite tener control perfecto y adecuado a cada una de las empresas ya que la versatilidad con la que consta esta herramienta hace posible la adaptación total o parcial a los diferentes ambientes que se la configure, con esto de una manera muy fácil puede llegar a convertirse en un SOC, permitiendo así un ahorro económico para la MiPymes en la que se implemente.

SOC significa Centro de Operaciones de Seguridad, que permite rastrear y monitorear los incidentes y la seguridad que ocurren en la organización.

Viabilidad

La principal posibilidad que se puede generar a base de este proyecto es la protección ante ataques maliciosos que puede presentarse dentro de una red de datos ya sea Domestica o MiPymes, brindando así una mejor protección y cuidado de la data que se maneje dentro de dicha red.

Impacto

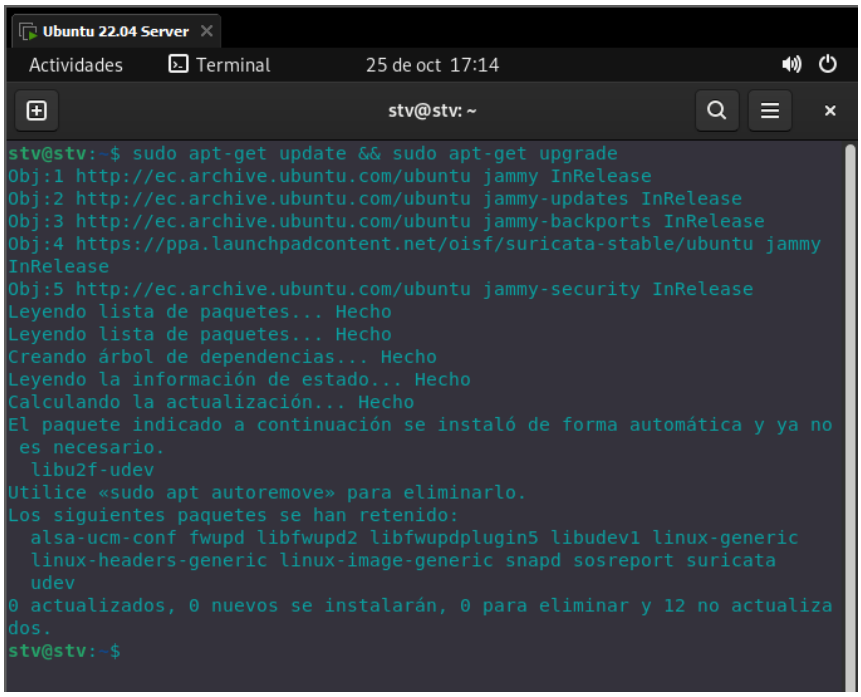
Acorde al resultado de las encuestas la mayoría de las empresas falla en la configuración perimetral, lo cual representa al primer bloqueo que se tiene dentro de una red, sin embargo, la mayoría estaría dispuesto a implementar seguridades con un porcentaje inferior a que debe pensarlo, esto implica que actualmente las empresas tienden a pensar ya en una ciberseguridad dentro de la compañía.

Desarrollo de la propuesta

La herramienta SURICATA tiene compatibilidad tanto para software libre (Linux) como para Windows, para el análisis se tomó la distribución de Ubuntu Server Linux versión 22.04.

Actualización de repositorios y librerías en Ubuntu Server 22.04 con el comando: ***-$ sudo apt-get update && sudo apt-get upgrade***

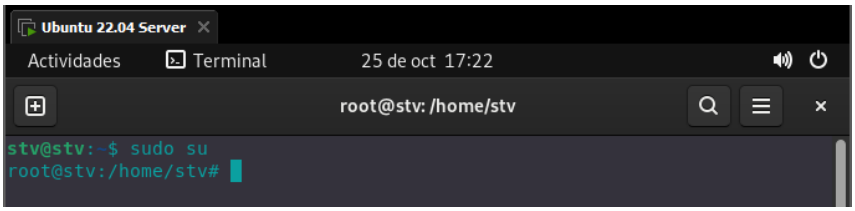
Figura 21:
Actualización de los repositorios de Ubuntu Server 22.04.



Nota: Se debe realizar una actualización en el sistema antes de instalar SURICATA para evitar inconvenientes con los repositorios.

Una vez actualizado el sistema operativo se procede a escalar los privilegios convirtiéndonos en super usuarios con el comando ***-$ sudo su*** para poder realizar la instalación de SURICATA.

Figura 22:
Escalamiento de privilegios.



Nota: El escalamiento de privilegios como super usuario, permite el acceso, modificación y configuración de los repositorios.

Posteriormente realizada el escalamiento adecuado de privilegios se procede a instalar la última versión disponible de SURICATA, mediante la adición del repositorio de SURICATA con el comando ***# add-apt-repository ppa:oisf/suricata-stable***

Figura 23:
Instalación de la herramienta de seguridad SURICATA.

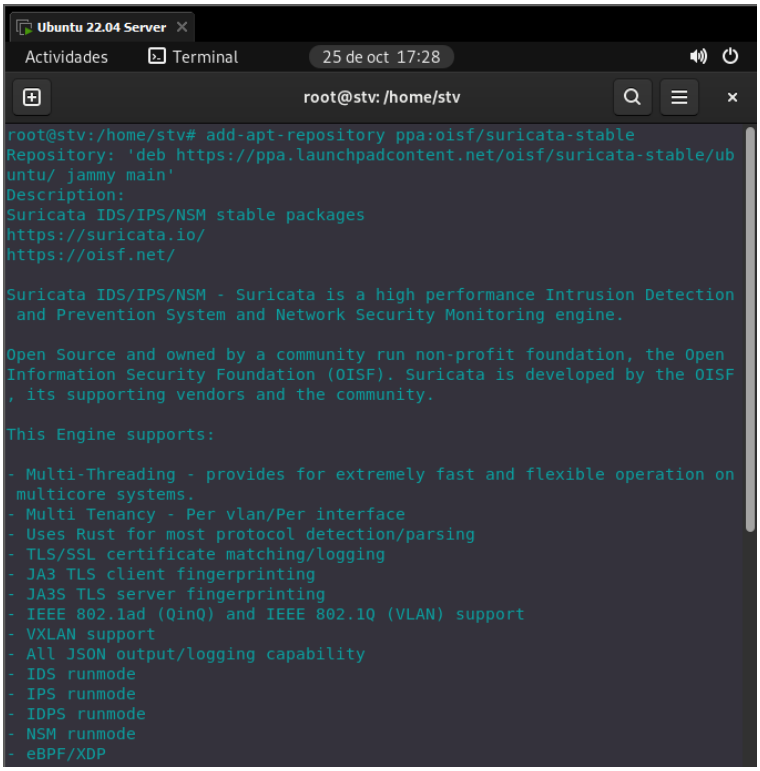


Figura 23.1:
Instalación de la herramienta de seguridad SURICATA.

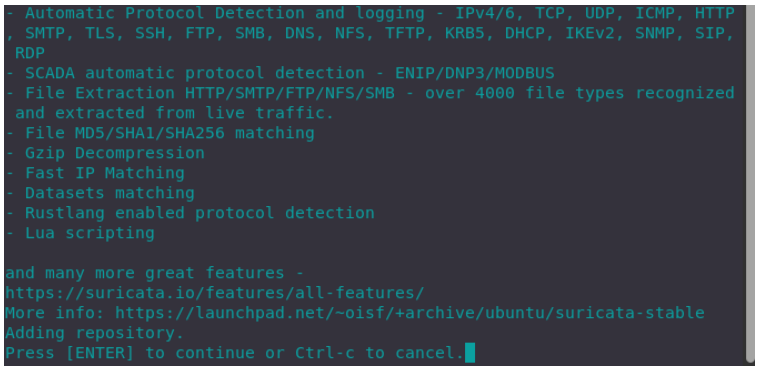
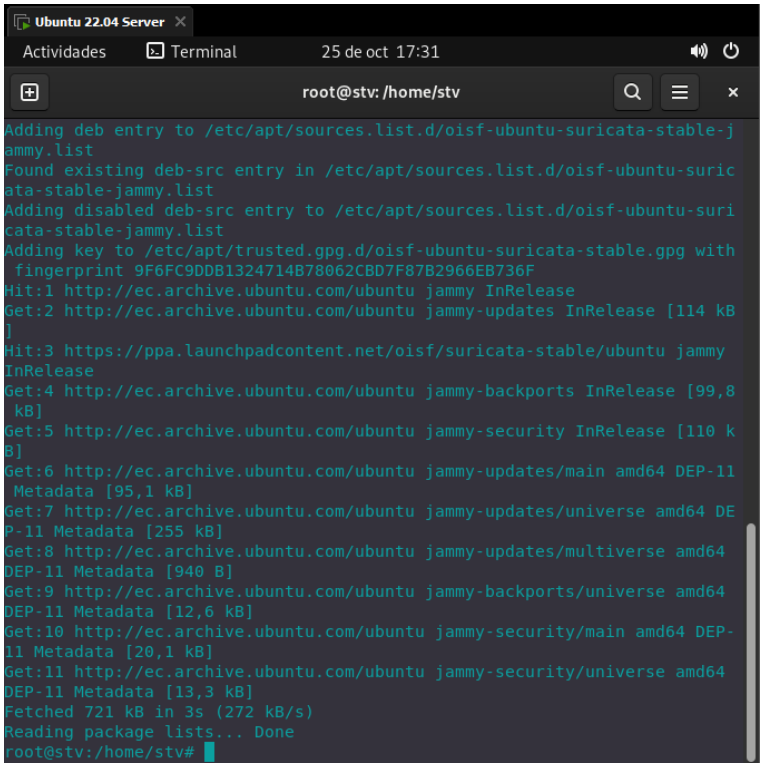


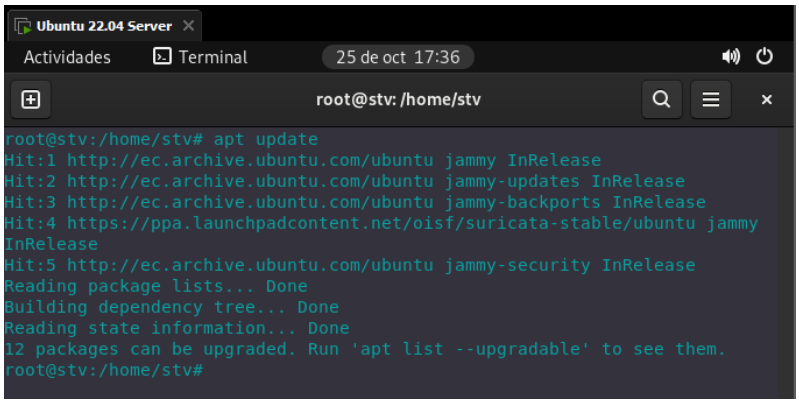
Figura 23.2:
Instalación de la herramienta de seguridad SURICATA.



Nota: En la figura 23.1, se debe confirmar con la tecla intro para continuar con la correcta instalación de SURICATA.

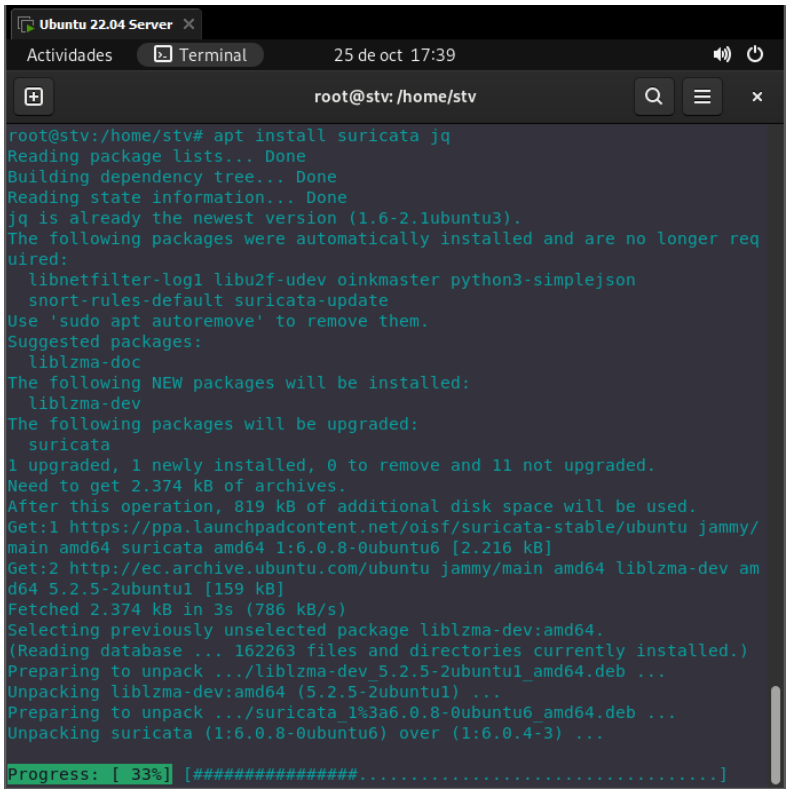
Una vez obtenido y añadido se actualiza nuevamente los repositorios con el comando ***# apt update***.

Figura 24:
Actualización de los paquetes del sistema.



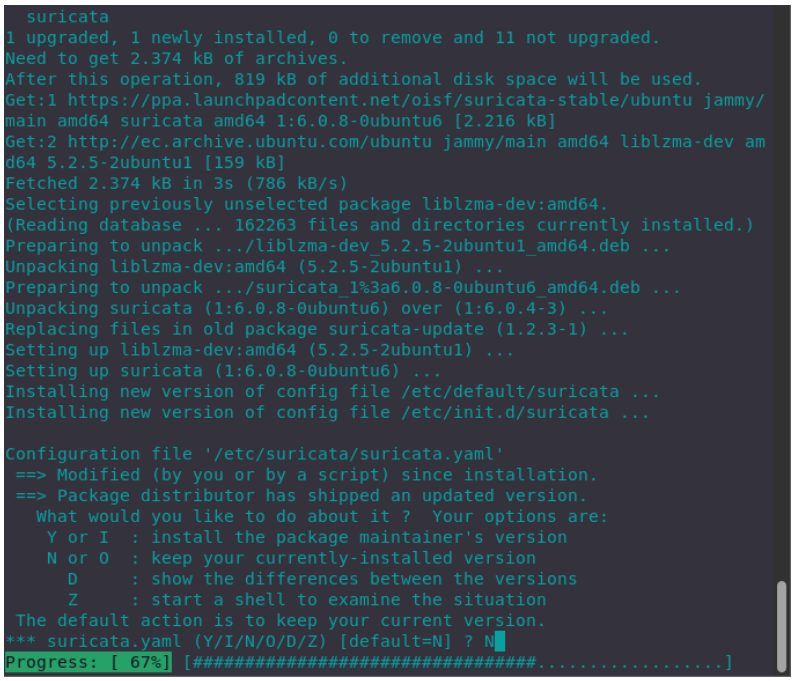
Con los paquetes actualizados se procede a instalar tanto SURICATA como SURICATA JQ el cual es un lector de registros que utiliza SURICATA para luego realizar con el comando ***# apt install suricata jq***

Figura 25:
Instalación de los repositorios de SURICATA y SURICATA JQ.



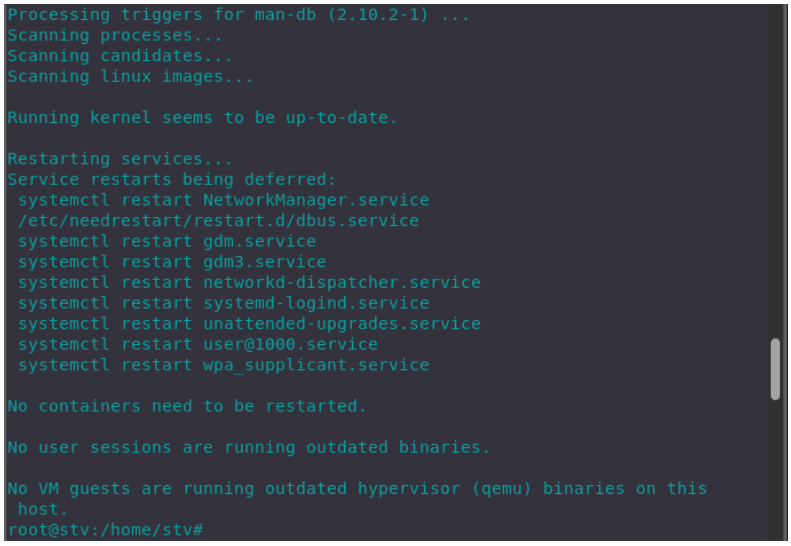
Nota: SURICATA JQ es un intérprete de archivos JSON.

Figura 25.1:
Instalación de los repositorios de SURICATA y SURICATA JQ.



Nota: En la figura 25.1 se debe colocar N para que mantenga la versión actual de SURICATA.

Figura 25.2:
Instalación de los repositorios de SURICATA y SURICATA JQ.



Se valida que la instalación fue realizada satisfactoriamente con el comando ***# whereis suricata*** el cual nos indica cual es el directorio de SURICATA.

Figura 26:
Confirmación de la instalación exitosa de SURICATA con un "Donde esta".

Nota: Para confirmar que SURICATA fue instalado correctamente debe indicarnos las dos rutas donde se encuentran los paquetes de SURICATA.

A continuación, se valida cuál es la configuración que mantiene SURICATA y el estatus con el comando #suricata –build-info && service suricata status.

Figura 27:
Validación de que SURICATA este activo y que los servicios más importantes en especial NFQueue estén corriendo.

Figura 27.1:
Validación de que SURICATA este activo y que los servicios más importantes en

especial NFQueue estén corriendo.

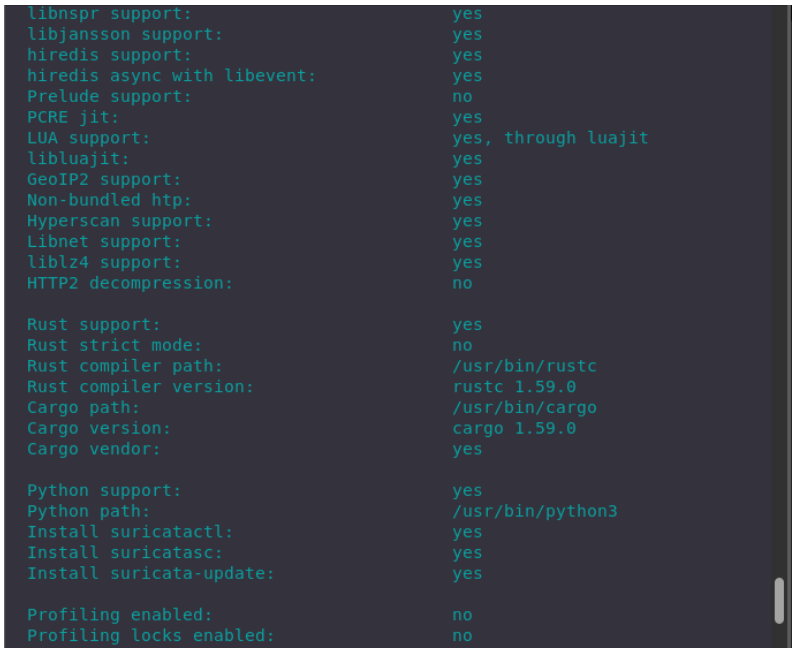
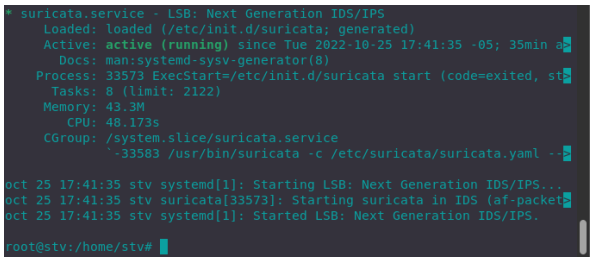


Figura 27.2:
Validación de que SURICATA este activo y que los servicios más importantes en

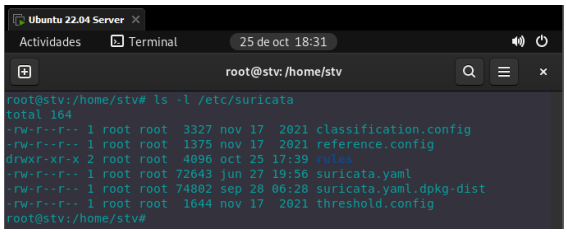
especial NFQueue estén corriendo.

Figura 27.3:
Validación de que SURICATA este activo y que los servicios más importantes en especial NFQueue estén corriendo.



Consecutivamente realizado estas acciones de comprobación se ejecuta una configuración en los ficheros de suricata recordando que estos ficheros se albergan en los ***paths: /usr/bin/suricata; /usr/lib/suricata; y /etc/suricata***, Se inicia verificando que es lo que contiene el directorio /etc/suricata con el comando ***# ls -l /etc suricata*** en el que consta con el fichero de rules y se realiza las modificaciones posteriormente.

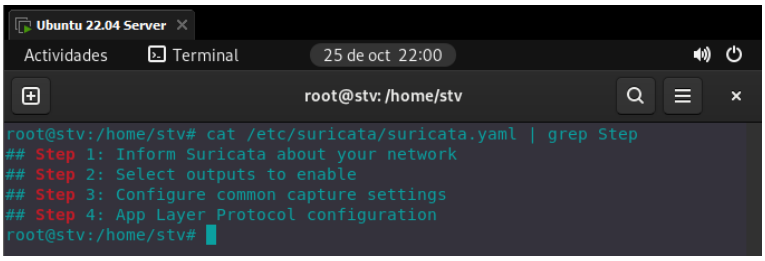
Figura 28:
Búsqueda del fichero que contiene las reglas de SURICATA en el directorio /etc/suricata.



Se visualiza el fichero de ***suricata.yaml*** en cual contiene los 4 pasos de la configuración de SURICATA, estos pasos son:

- **Paso1:** Informe de suricata sobre la red,
- **Paso2:** Selección de las salidas,
- **Paso3:** Configuración de ajuste de capturas comunes,
- **Paso4:** Configuración del protocolo de la capa de aplicación.

Figura 29:
Revisión del fichero suricata.yaml, donde se realizaran las configuraciones de las nuevas reglas y directorios.

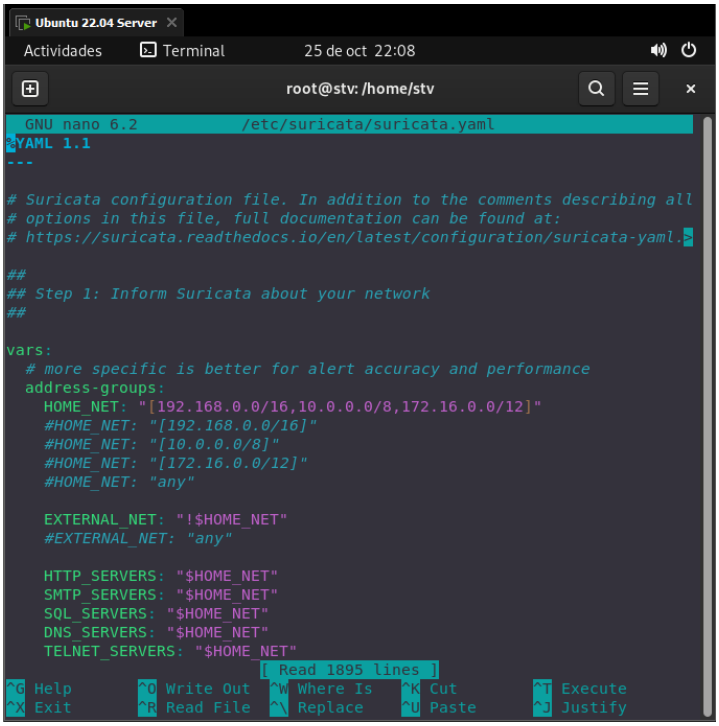


Nota: Se usa el comando CAT para la lectura y validación del fichero.

Se ingresa al fichero para editar con el comando ***# nano /etc/suricata/suricata.yaml***, en el cual se procede a ir paso por paso (step by step) configurando acorde nuestra infraestructura así lo requiera.

En el primer paso se configura el segmento de red el cual va a ser monitoreado por SURICATA, todo esto se aplica a la versión IPv4.

Figura 30:
Revisión del fichero suricata.yaml, donde se realizaran las configuraciones de las nuevas reglas y directorios.

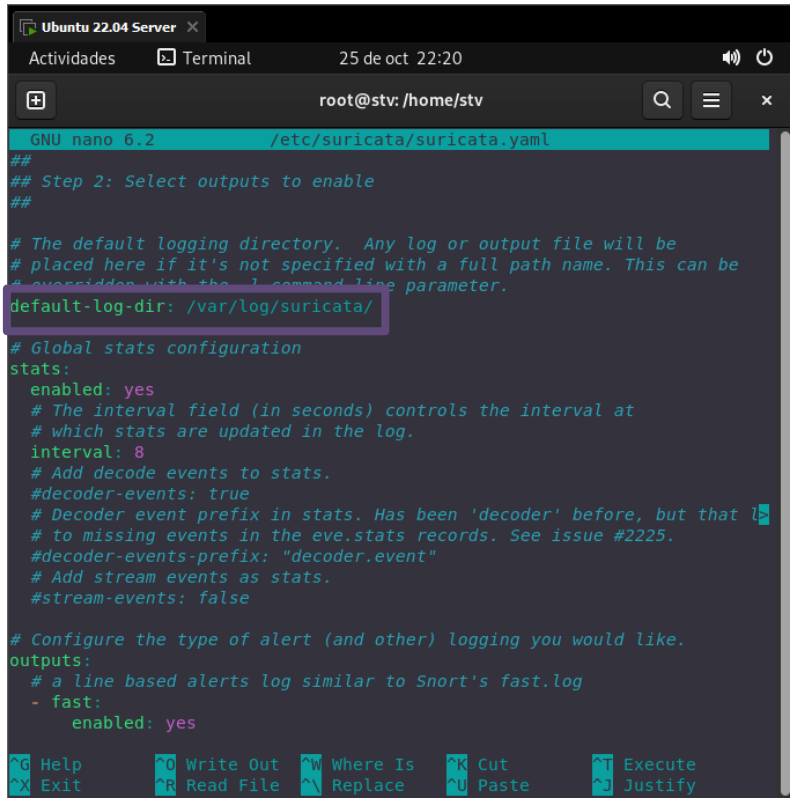


Nota: Se usa el comando NANO para la edición del fichero.

En esta configuración se puede visualizar que en la parte de la declaración de variable “grupo de direcciones” en el apartado de red domestica (**HOME_NET**), hay varias configuraciones las cuales se puede comentar y descomentar acorde al criterio del especialista y segmento de red que se tenga, en la parte de red externa (**EXTERNAL_NET**) se refiere a todo lo que no esté –dentro del home net esto se puede aplicar de mejor forma cuando existe un segmento más establecido (rango de ip a monitorear).

En el segundo paso, lo que interesa revisar que este bien configurado es los registros de logueo (**LOG**).

Figura 31:
Validación del directorio donde se encuentra albergado los logs de SURICATA.

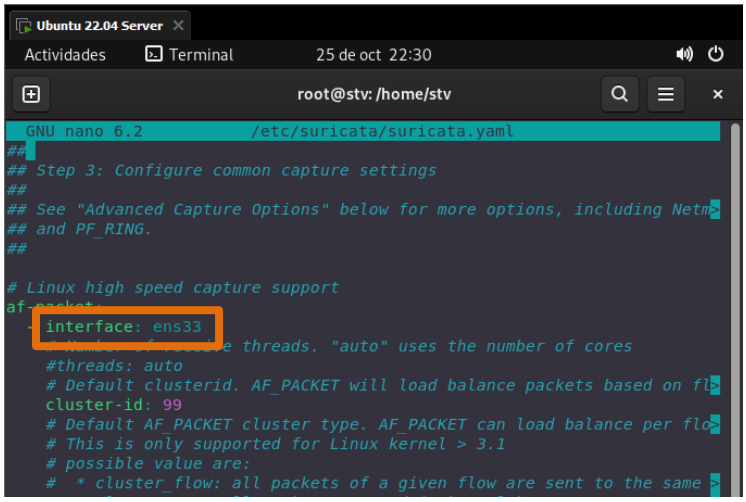


En estos registros se almacenan los registros o historiales de todos los acontecimientos o eventos (acciones) que se realizan dentro de la red, en este caso

es el lugar donde se van a encontrar todas las incidencias o eventos fortuitos (ataques a la integridad) que ocurran dentro de la red.

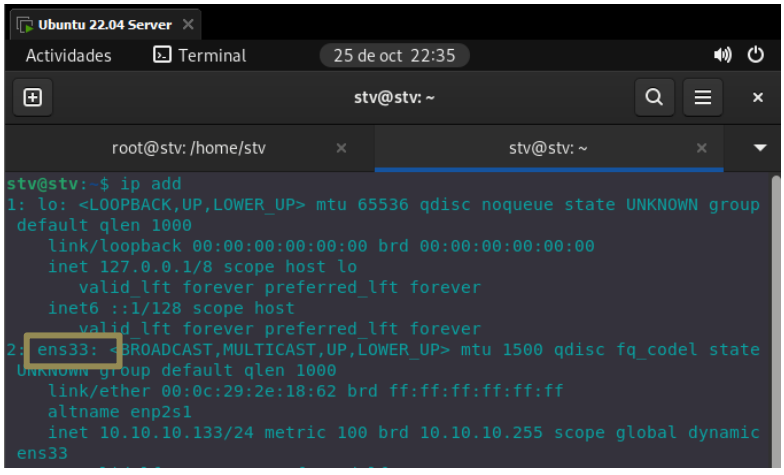
En el tercer paso, es donde se configura el “donde se va a realizar el análisis”.

Figura 32:
Comprobación de la interfaz de red por donde se va a comunicar SURICATA.



Se valida cual es la interfaz por la cual va a realizar el análisis SURICATA, para esto en otra terminal se procede a confirmar cual es la interfaz de red que existe a fin de que se haga el monitoreo con SURICATA.

Figura 33:
Comprobación de la interfaz de red.



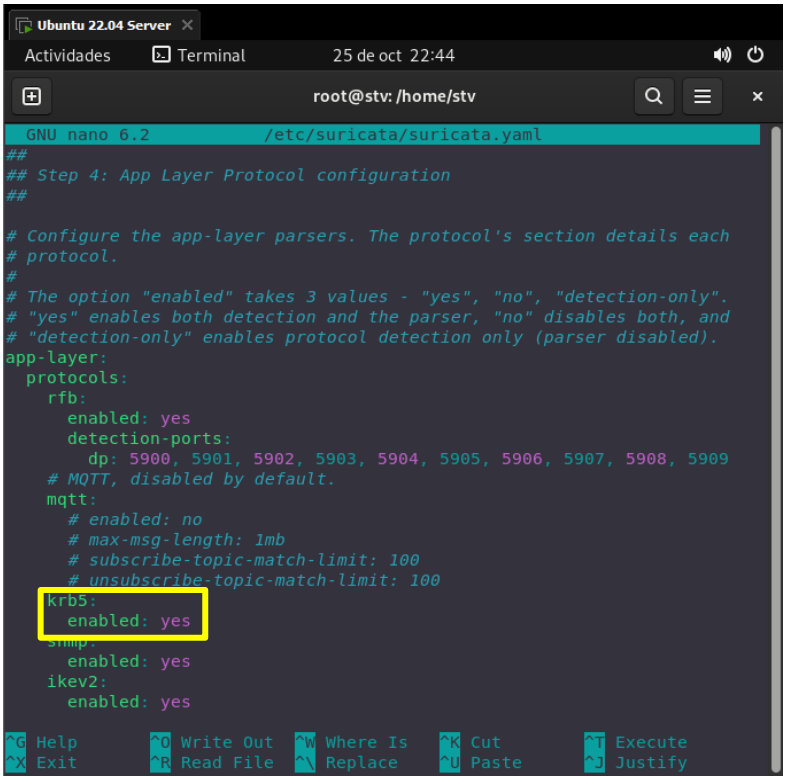
Nota: En una nueva terminal con el comando IP ADD se valida cual es la interfaz de red.

Una vez ya confirmado que el nombre de la interfaz es la correcta con la configuración del paso 3. Este paso llega a ser uno de los más importantes debido a que si no se coloca el puerto de escucha adecuado SURICATA no va a funcionar correctamente y no proporcionara toda la data y análisis de lo que suceda dentro de la red en la cual se está configurando.

Por último, se realiza una validación y posterior configuración si así se requiere de los puertos y protocolos los cuales van a realizar las detecciones en la red, todo esto se puede configurar el cuarto paso.

En este paso se puede visualizar que se encuentra habilitado la detección del protocolo ***KERBEROS*** el cual sirve para realizar autenticaciones primordialmente del modelo cliente-servidor.

Figura 34:
Comprobación del estatus de los protocolos en SURICATA.

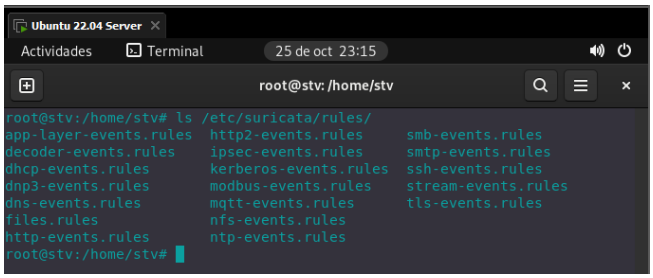


Nota: En este punto se valida que los protocolos de seguridad estén activos como lo es KERBEROS.

Una vez realizado todas estas configuraciones se guardan los cambios realizados y salir del fichero. Con estos ajustes queda realizado las configuraciones generales de SURICATA.

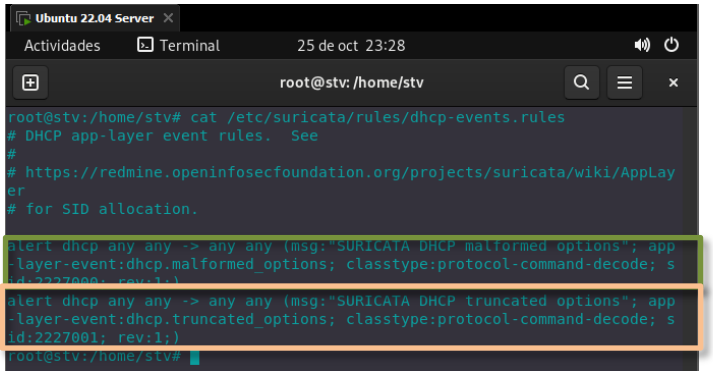
Posterior a esto se realiza las configuraciones de las reglas (***RULES***), con el comando ***# ls /etc/suricata/rules/*** listamos todos los ficheros existentes.

Figura 35:
Listado de los ficheros de SURICATA albergados dentro del directorio ***/etc/suricata/rules.***



El fichero que se va a visualizar como ejemplo es el de ***dhcp-events.rules*** con el comando ***# cat /etc/suricata/rules/dhcp-events.rules***.

Figura 36:
Lectura del fichero ***dhcp-events.rules****.*



Se puede visualizar las dos reglas que están albergadas en este fichero. Estas reglas son compatibles con otros sistemas de IDS/IPS tales como ***SNORT***, lo cual hace más fácil el uso y configuración (importación y exportación) de las reglas.

Haciendo un detalle más a profundidad de que son las reglas se explica con un ejemplo de su composición y su funcionamiento.

Tabla 3:
Tabla de composición de las reglas de SURICATA.

• **reject ip 192.168.10.0/24 80 -> 92.69.20.0/26 80 (msg:“Mensaje log”; sid:10001; rev:1;)**
• **alert icmp any any -> any any (msg:”ICMP Packet found”; sid:2000001; rev:1;)**
• **drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:”ET TROJAN Likely Bot Nick in IRC (USA +..)”; Flow:established,to_server, flowbits:isset,is_proto_irc; content:”NICK”; pcre:”/NICK .*USA.*[0-9]{3,}/i”; reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity; sid:2008124; rev:2;)**

Tabla 4:
Tabla de formato de las reglas de SURICATA.

●	Acción:	alert, pass, drop, reject...
●	Encabezado:	[protocolo Origen IP puerto Sentido Destino IP puerto]
●	Opciones de regla:	<keyword>: <settings>; <keyword>;

La acción se compone de una sola palabra y esta es la que indica cual es la acción a tomar dentro del paquete, lo que quiere decir que esto determina si se va a crear una alerta, si se rechaza, si se elimina el paquete.

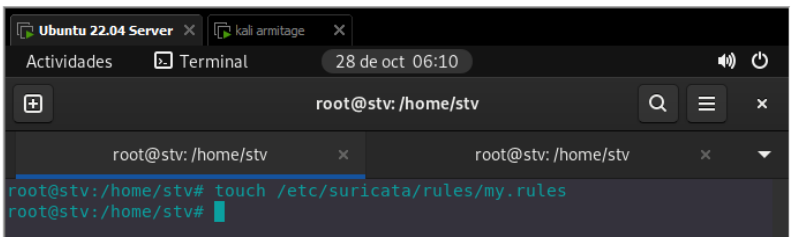
Lo siguiente es el encabezado en el que se incluye el protocolo, la dirección origen, el puerto origen, sentido de la comunicación, la dirección ip destino y el puerto de origen. El sentido de la comunicación tiene solo dos vías la primera es **fuente -> destino** (source -> destination) en un solo sentido y por último **fuente <> destino** (source <> destination) ambos sentidos; no existe la manera que sea en el

sentido “inverso” de **destino <- fuente** (destination <- source) por motivos de que nuestra salida de paquetería no afecta a las reglas de entrada que se va a configurar.

Por último, existen las opciones de regla, estas opciones varían no son de tamaño fijo esto quiere decir que podemos añadir y configurar acorde al propósito, estas reglas se basan por el protocolo que se esté utilizando, la sintaxis definida para que una regla funciones es la siguiente: entre paréntesis debe ir la palabra clave <keyword> ej: msg, seguido de un ajuste <settings>, este ajuste puede variar siempre y cuando la palabra clave lo permita, esto puede aplicarse las veces que sean necesarias, es decir: **(<keyword>; <settings>; <keyword>;<settings>; <keyword>;)**, siempre separando las opciones de regla con punto y coma (;), es importante recordar que hay palabras (keywords) que no requieren de ninguna configuración, tal es el caso de la **keyword nocase** la cual hace referencia a que no discrimine si es mayúscula o minúscula.

En este punto se procede a la creación del fichero personal en el cual van a constar las reglas que se va a implementar dentro de SURICATA, este fichero llevara por nombre ***“my.rules”*** el cual va a estar ubicado en el siguiente path: ***/etc/suricata/rules/***

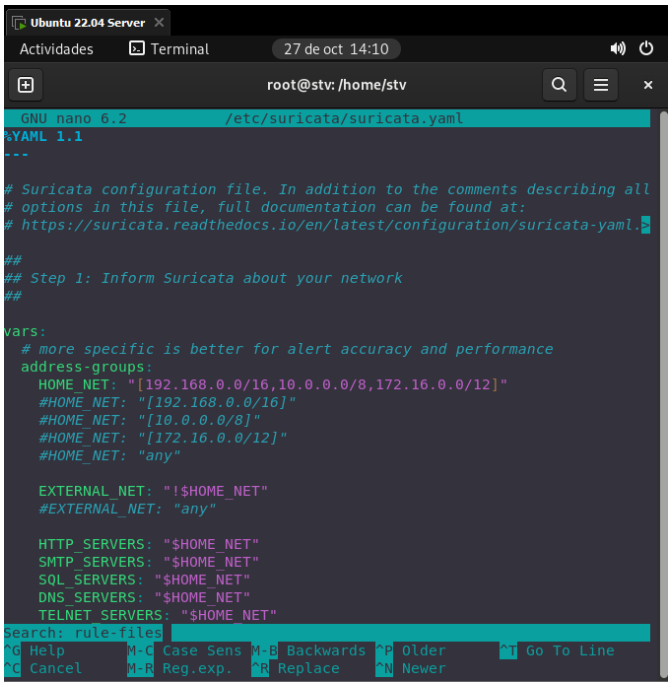
Figura 37:
Creación de un nuevo fichero membretado **my.rules**.



Nota: Con el comando TOUCH se crea un nuevo archivo.

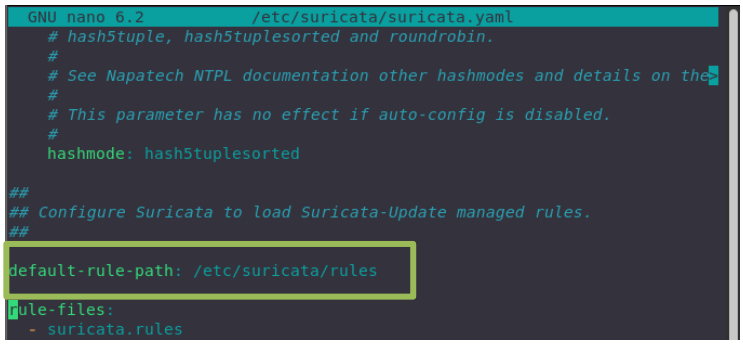
A continuación, se debe ingresar el fichero de configuración principal (general), en el cual se indexan las nuevas rutas de las reglas que se acaban de crear.

Figura 38:
Validación de las rutas existentes dentro del archivo de configuración general.



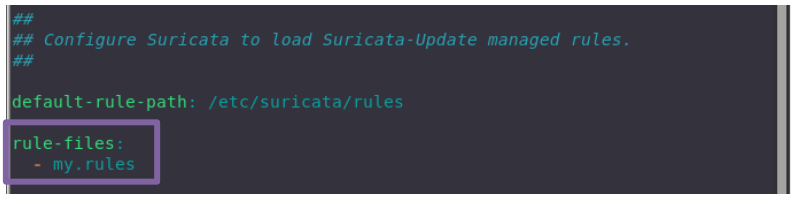
El primer cambio a realizar es el directorio por defecto de las reglas de SURICATA, en el cual se colocará el path correspondiente el cual es: ***/etc/suricata/rules.***

Figura 39:
Cambio del directorio anterior al nuevo en donde se encuentra el archivo creado anteriormente.



Posterior a este cambio se coloca el nombre del fichero que va a contener las nuevas reglas.

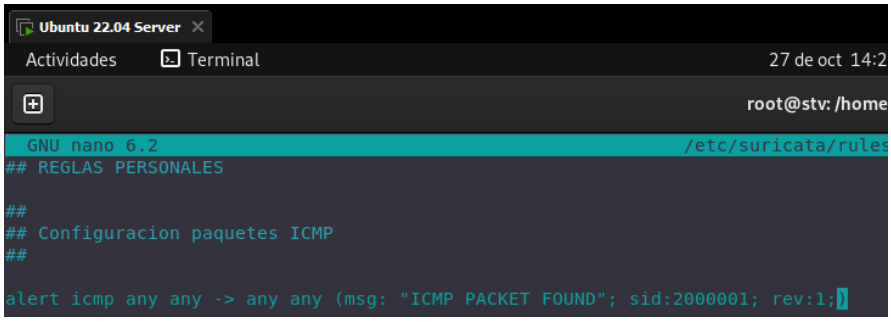
Figura 40:
Cambio del nombre del fichero anterior por el que se ha creado.



Los cambios realizados se proceden a guardar y se accede al fichero que van a contener las reglas.

La primera regla a ser creada es la detección de paquetes ICMP.

Figura 41:
*Creación de la primera regla dentro del fichero **my.rules**.*



Se guarda el primer cambio, y reinicia el servicio de SURICATA con ***#service suricata restart*** para que pueda leer la nueva configuración realizada dentro del fichero.

Figura 42:
Puesta en marcha del servicio de SURICATA.

Nota: Se debe resetear el servicio de suricata siempre que se realicen cambios dentro de los ficheros para que se acople a los cambios realizados.

A la par se abre una nueva terminal en donde se indicará todo el flujo de incidencias que ocurra dentro del fichero de ***fast.***log con el comando ***tail -f*** en el directorio ***/var/log/suricata/fast.log***

Figura 43:
Revisión de los logs registrados por incidencias dentro de la red.

Nota: Con el comando TOUCH se crea un nuevo archivo.

Se hace la comprobación de que la regla funcione adecuadamente haciendo un ping desde el equipo atacante (***Kali Linux***) hacia el servidor de SURICATA.

Figura 44:
Realización de un ICMP o ping exitoso, desde la maquina atacante.

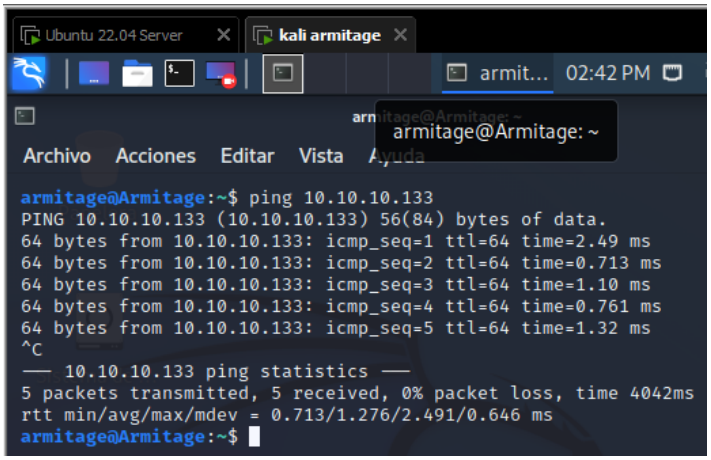
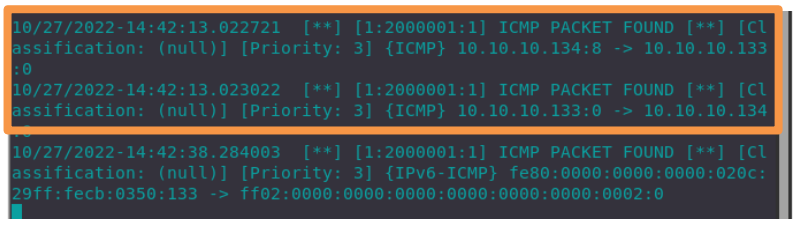


Figura 45:
Revisión de las alertas en el fichero fast.log por un ping enviado desde una máquina.



Seguidamente se crea la siguiente regla que es la detección de conexiones TCP, en este caso se ha creado tres reglas para cada una de los aplicativos webs más comunes que son: Facebook e Instagram.

Figura 46:
Creación de las reglas para el bloqueo de redes sociales.

```
##
## Configuracion paquetes TCP ##
##

drop tcp any any -> any any (msg: "FB esta bloqueado"; content:"facebook"; sid:1000002; rev:1;)
drop tcp any any -> any any (msg: "ING esta bloqueado"; content:"instagram"; sid:1000003; rev:1;)
```

Se comprueba el correcto funcionamiento de la nueva regla, mediante un ***CURL***.

Figura 47:
Mediante curl -i se valida la conexión a las redes sociales.

```
stv@stv:~$ curl -i instagram.com
HTTP/1.1 301 Moved Permanently
Location: https://instagram.com/
Content-Type: text/plain
Server: proxygen-bolt
X-FB-TRIP-ID: 1679558926
Alt-Svc: h3=":443"; ma=86400
Date: Mon, 31 Oct 2022 04:24:05 GMT
Connection: keep-alive
Content-Length: 0

stv@stv:~$ curl -i facebook.es
HTTP/1.1 302 Found
Location: https://es-es.facebook.com/
Content-Type: text/html; charset="utf-8"
X-FB-Debug: xEdiGcSFAojPAoHrkScg4et67iZ1zIna05bc7YnMJ
Date: Mon, 31 Oct 2022 04:24:21 GMT
Alt-Svc: h3=":443"; ma=86400
Connection: keep-alive
Content-Length: 0
```

Nota: El comando CURL permite una conexión directa con servidores y API mediante CLI.

Figura 48:
Revisión en el fichero fast.log.

```
root@stv:/home/stv# tail -f /var/log/suricata/fast.log
10/30/2022-23:24:05.513946  [wDrop] [**] [1:1000003:1] ING esta bloqueado
 [**] [Classification: (null)] [Priority: 3] {TCP} 10.10.10.133:46112 ->
31.13.67.174:80
10/30/2022-23:24:21.546394  [wDrop] [**] [1:1000002:1] FB esta bloqueado
[**] [Classification: (null)] [Priority: 3] {TCP} 10.10.10.133:51284 -> 1
57.240.14.15:80
```

A pesar de que estas páginas manejen protocolo cifrado como es HTTPS, se puede obtener el mensaje de alerta por motivo de que el encabezado es público.

Continuando con la creación de la tercera regla de peticiones GET, se va a crear una regla la cual va a contener variables establecidas y puertos específicos; utilizando de la misma forma una keyword la cual será ***FLOW*** que sirve para las peticiones cliente–servidor en donde indicará si está establecido o no, y de la misma forma que el contenido sea un método http.

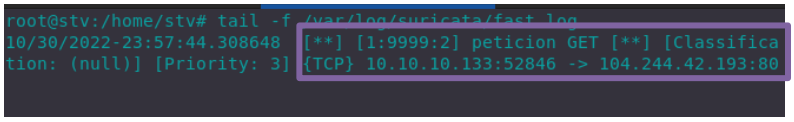
Figura 49:
Creación de la regla para peticiones get.

Realización de la prueba de igual forma como en la regla anterior con un curl.

Figura 50:
Mediante curl -i se valida la petición a un servicio en la web.

Se comprueba que está funcionando la regla de una manera correcta.

Figura 51:
Comprobación del correcto funcionamiento de la regla en el fichero fast.log



Se puede evidenciar que la petición GET realizada desde la ip origen hacia la ip destino fue realizada con éxito.

La creación de la cuarta regla es la detección de conexiones SSH, con una configuración ***any any*** hacia ***any 22*** lo que indica que desde cualquier ip y cualquier puerto hacia cualquier ip que contenga el puerto 22 indica que se están tratando de conectar, y bote la alerta.

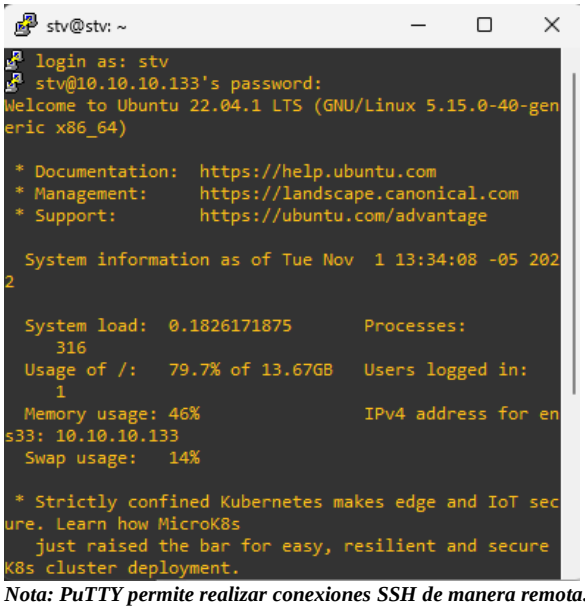
Figura 52:
Creación de la regla para conexiones SSH.

```
##
## Configuracion paquetes SSH ##
##

alert tcp any any -> any 22 (msg:"Conexion SSH Detectada"; flow:to_serve
```

Realizando una prueba por PuTTY se validará el funcionamiento apropiado de la regla creada.

Figura 53:
Conexión hacia el servidor Ubuntu 22.04 mediante PuTTY.



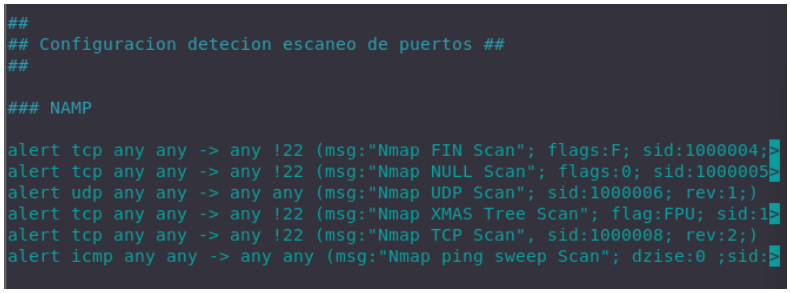
Nota: PuTTY permite realizar conexiones SSH de manera remota.

Figura 54:
Comprobación del correcto funcionamiento de la regla en el fichero fast.log

```
root@stv:/home/stv# tail -f /var/log/suricata/fast.log
11/01/2022-13:32:45.447929  [**] [1:2271009:1] Conexion SSH Detectada [**] [Classification: (null)] [Priority: 3] {TCP} 10.10.10.1:54251 -> 10.10.10.133:22
```

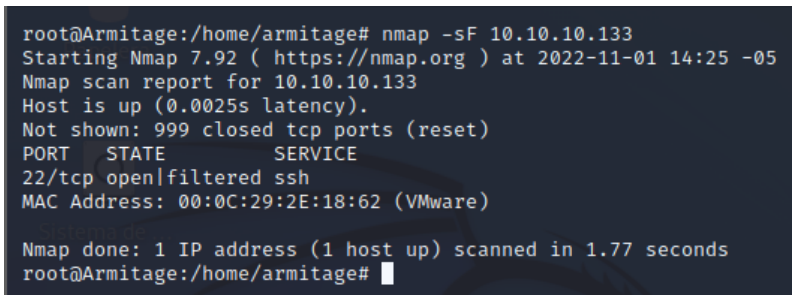
La regla a ser creada a continuación es el bloqueo de un escaneo de puertos por medio de NMAP

Figura 55:
Creación de la regla para detección de un escaneo de puertos.



Con este equipo atacante se realizará una prueba de escaneo de puertos mediante la bandera ***-sF.***

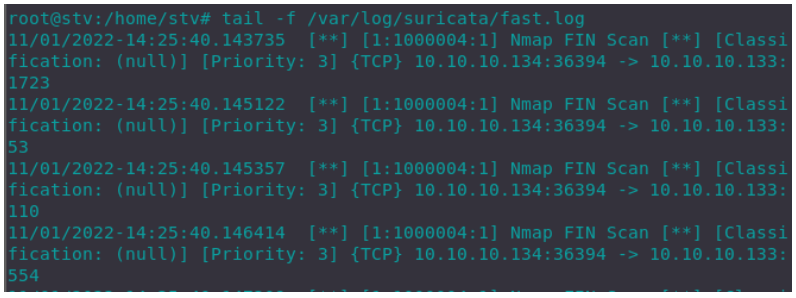
Figura 56:
Escaneo de puertos desde la maquina atacante mediante NMAP.



Nota: La bandera -sF permite hacer un bypass en el firewall.

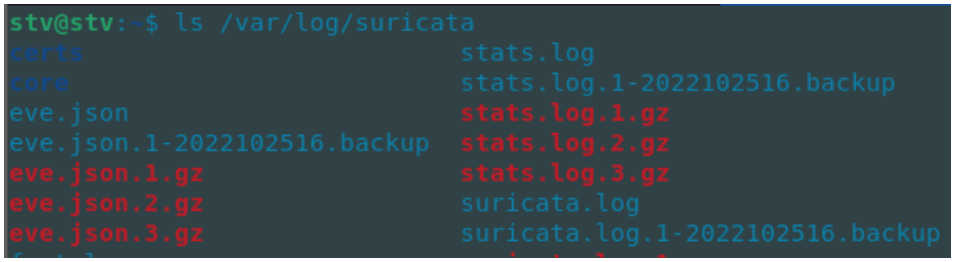
Se puede evidenciar como la regla que contiene los campos de detección para el tipo de escaneo ***"Nmap ping sweep scan"*** está detectando correctamente.

Figura 57:
Comprobación del correcto funcionamiento de la regla en el fichero fast.log



De la misma manera se puede realizar un análisis de la información con **JQ**, SURICATA no solo permite visualizar la información en formato Desktop si no también lo registra en formato JSON, como se muestra en los registros:

Figura 58:
Listado de los registros de los ficheros en formato JSON.



Se lee el fichero ***eve.json*** nos indica la información en forma masiva tal cual es el formato json.

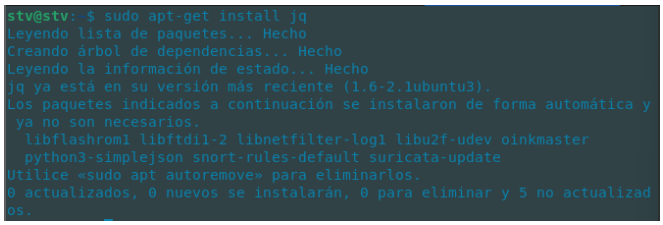
Figura 59:
Lectura de un fichero en formato JSON.

Nota: Se visualiza de esta forma la información debido a que no está instalada JQ.

Con esta herramienta JQ permite visualizar toda esta información de forma más entendible y para esto se debe instalar JQ de la siguiente manera:

Figura 60:

Instalación de la herramienta JQ.



Para hacer uso de la herramienta JQ es menester realizarla mediante: "***tail /var/log/suricata/eve.jason | jq '.'***", el cual tiene un funcionamiento similar como el comando **grep.** De tal forma que ahora indica toda la información del fichero "***eve.json***" de una manera ordenada y más estética al vista.

Figura 61:
Lectura del fichero **eve.json** mediante la herramienta JQ.

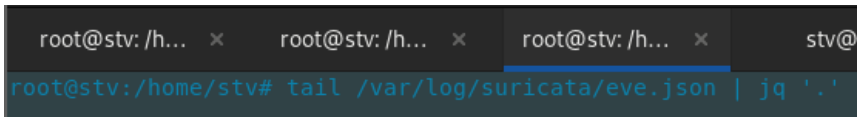
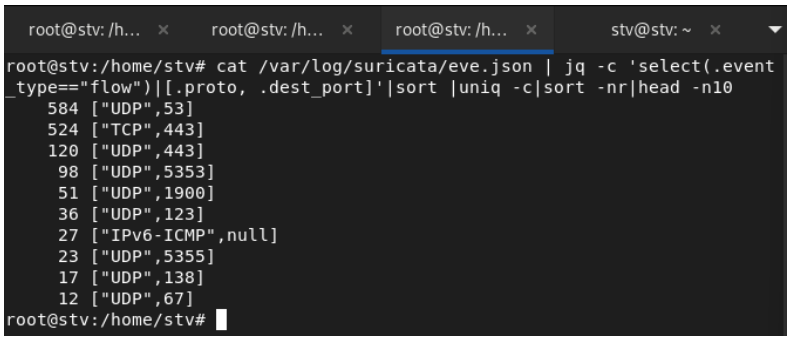


Figura 61.1:
Lectura del fichero **eve.json** mediante la herramienta JQ.

Nota: JQ permite tener toda la información de manera vertical para su fácil lectura y entendimiento.

JQ tiene un sin número de utilidades las cuales permite filtrar la información para poder analizar de una mejor manera, como es el caso de: "***cat /var/log/suricata/eve.jason | jq -c 'select(.event_type=="flow")|[.proto, .dest_port]'|sort |uniq -c|sort -nr|head -n10***" en el cual indica de los registros que mantiene los últimos 10 puertos en orden que ha detectado.

Figura 62:
Validación de los 10 puertos más usados con la herramienta JQ.

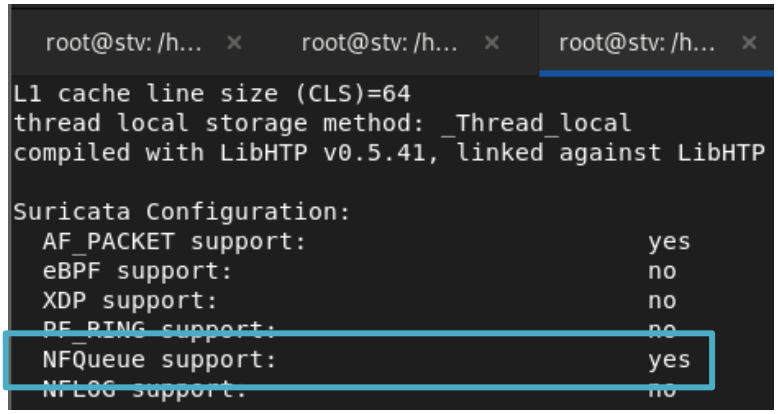


Hasta el momento se ha realizado la configuración de SURICATA en modo IDS, lo cual ha permitido detectar y analizar el tráfico como un agente pasivo y registrarlo en un fichero sin realizar ninguna acción sobre este tráfico.

Ahora se configurará SURICATA como un IPS, para que pueda tomar decisiones como bloquear el tráfico no deseado.

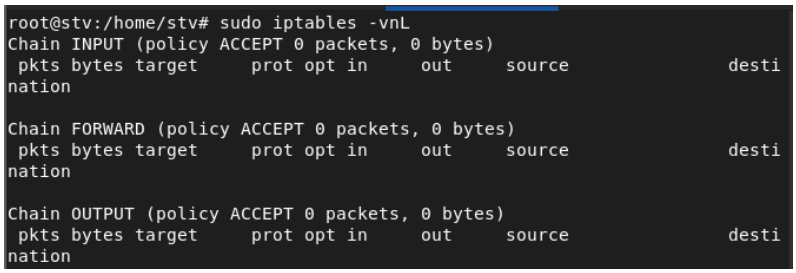
El primer paso es verificar que SURICATA tenga habilitado ***"NFQ"***, lo cual se realiza con el comando "***suricata –build-info***".

Figura 63:
*Verificación de que **NFQueue** este activado.*



Una vez realizada la comprobación se debe modificar las "***IPTABLES***", ya que se debe realizar un **BYPASS** en las **IPTABLES**, las mismas que son las que vienen por defecto instaldas en el kernel de Linux.

Figura 64:
Revisión de las IPTABLES propias de Ubuntu server 22.04.

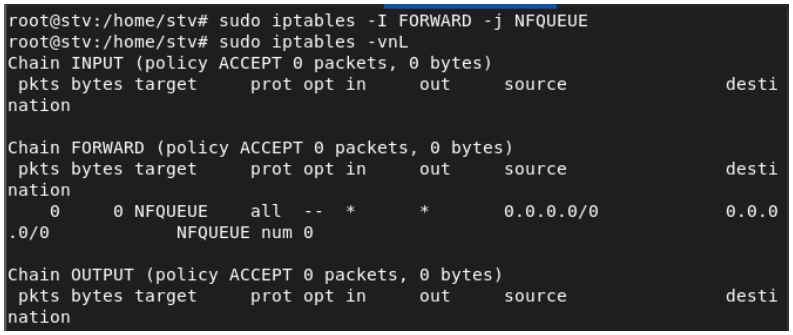


Debido a que el cortafuegos se divide en tres reglas distintas las cuales son:

- **INPUT:** El tráfico que ingresa en el equipo.
- **FORWARD:** El tráfico que pasa por el equipo.
- **OUTPUT:** El tráfico que sale del equipo o que genera el equipo.

Se debe configurar cada una de ellas la primera es ***"FORWARD"***, esto se realiza con: "***sudo iptables -I FORWARD -j NFQUEUE***".

Figura 65:
Configuración de las IPTABLES "forward" y redireccionamiento hacia SURICATA.



Como SURICATA está configurada como HOST, se debe configurar para que recepte todo el tráfico que ingresa y sale del equipo y esto se realiza con los comandos:

- ***sudo iptables -I INPUT -j NFQUEUE***
- ***sudo iptables -I OUTPUT -j NFQUEUE***

Figura 66:
Configuración de las IPTABLES "input, output" y redireccionamiento hacia SURICATA.

```
root@stv:/home/stv# sudo iptables -I INPUT -j NFQUEUE
root@stv:/home/stv# sudo iptables -I OUTPUT -j NFQUEUE
root@stv:/home/stv# sudo iptables -vnL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               desti
nation
    0     0 NFQUEUE    all  --  *      *       0.0.0.0/0            0.0.0
.0/0            NFQUEUE num 0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               desti
nation
    0     0 NFQUEUE    all  --  *      *       0.0.0.0/0            0.0.0
.0/0            NFQUEUE num 0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               desti
nation
    0     0 NFQUEUE    all  --  *      *       0.0.0.0/0            0.0.0
.0/0            NFQUEUE num 0
```

Nota: Las IPTABLES son las reglas del Firewall propio del servidor.

Con estas configuraciones se indica que sin importar el tráfico que ingrese o salga (origen-destino), pase todo por SURICATA.

Posterior a la configuración de las IPTABLES, se debe configurar las reglas haciendo un cambio en las reglas que indican **ALERT** por **DROP**

Figura 67:
Configuración de las reglas creadas en los pasos anteriores.

```
##
## Configuracion paquetes ICMP ##
##

drop icmp any any -> any any (msg: "ICMP PACKET FOUND"; sid:20

##
## Configuracion paquetes TCP ##
##

drop tcp any any -> any any (msg: "FB esta bloqueado"; content
drop tcp any any -> any any (msg: "ING esta bloqueado"; conten
```

Figura 67.1:
Configuración de las reglas creadas en los pasos anteriores.

```
### NAMP

drop tcp any any -> any !22 (msg:"Nmap FIN Scan"; flags:F; sid
drop tcp any any -> any !22 (msg:"Nmap NULL Scan"; flags:0; si
drop udp !10.10.10.133 any -> !10.10.10.133 any (msg:"Nmap UDP
drop tcp any any -> any !22 (msg:"Nmap XMAS Tree Scan"; flag:F
drop tcp any any -> any !22 (msg:"Nmap TCP Scan", sid:1000008;
drop icmp any any -> any any (msg:"Nmap ping sweep Scan"; dzis
```

De tal forma que ninguna de estas peticiones sea permitida y se pueda denegar todo el tráfico malicioso que cumpla con estas reglas.

Ya configurada resta lanzar SURICATA para que se actualice con la nueva configuración.

Finalmente se descargan las reglas de **"EMERGING THREATS"**, este es un proyecto comunitario de código abierto que tiene soporte constante con el cual se mantienen al día con todas las reglas y previenen la intrusión y amenazas en la red.

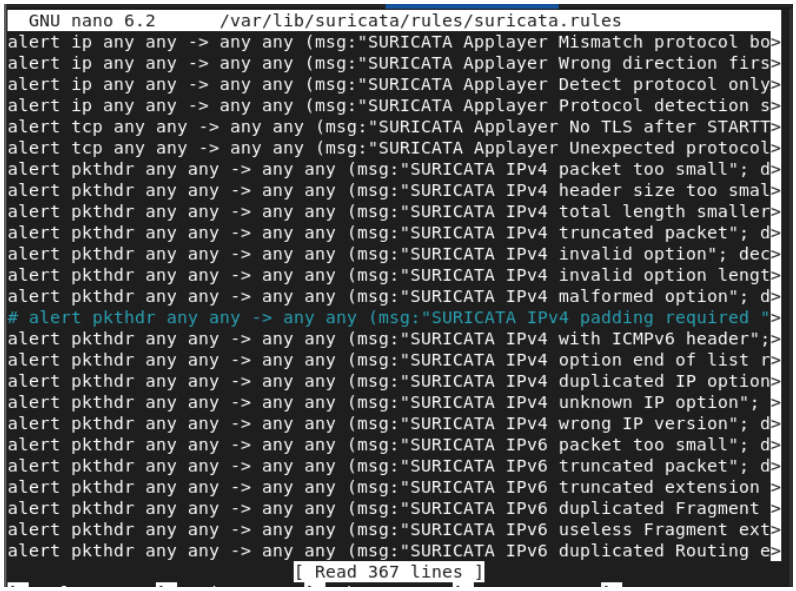
Para esto se debe descargar las ultimas actualizaciones de SURICATA con un update.

Figura 68:
Actualización de los repositorios de SURICATA.

```
stv@stv:~$ sudo suricata-update
7/11/2022 -- 14:45:06 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2022 -- 14:45:06 - <Info> -- Using Suricata configuration /etc/suric
ata/suricata.yaml
7/11/2022 -- 14:45:06 - <Info> -- Using /etc/suricata/rules for Suricata
provided rules.
7/11/2022 -- 14:45:06 - <Info> -- Found Suricata version 6.0.8 at /usr/bi
n/suricata.
7/11/2022 -- 14:45:06 - <Info> -- Loading /etc/suricata/suricata.yaml
7/11/2022 -- 14:45:06 - <Info> -- Disabling rules for protocol http2
7/11/2022 -- 14:45:06 - <Info> -- Disabling rules for protocol modbus
7/11/2022 -- 14:45:06 - <Info> -- Disabling rules for protocol dnp3
7/11/2022 -- 14:45:06 - <Info> -- Disabling rules for protocol enip
7/11/2022 -- 14:45:06 - <Info> -- No sources configured, will use Emergin
g Threats Open
7/11/2022 -- 14:45:06 - <Info> -- Fetching https://rules.emergingthreats.
net/open/suricata-6.0.8/emerging.rules.tar.gz.
```

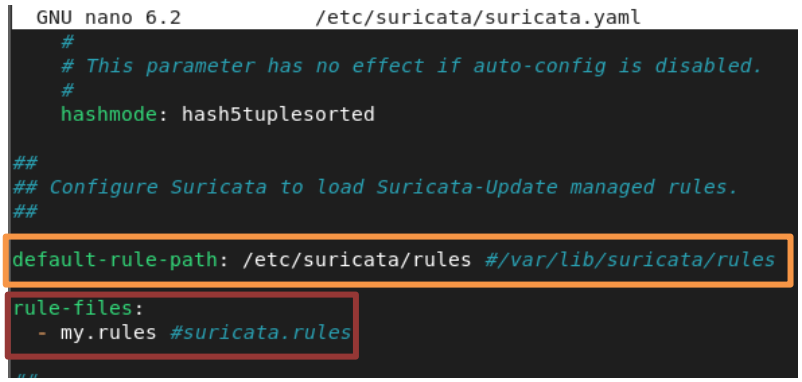
Actualizado suricata se valida el fichero con las nuevas reglas las cuales se encuentran en ***"/var/lib/suricata/rules/suricata.rules"***

Figura 69:
Revisión de las reglas por defecto que tiene SURICATA.



Las cuales nos indica que este fichero tiene 367 líneas con **ALERT.** Para que estas reglas funcionen se debe configurar en el fichero maestro.

Figura 70:
Configuración del fichero suricata.yaml, inserción del nuevo directorio y archivo.



Nota: Las librerías añadidas al fichero maestro sirve para tener como respaldo dado que se deba hacer algún mantenimiento o corrección dentro de nuestro fichero de reglas.

Síntesis del capítulo

Este capítulo cubre la parte práctica del proyecto y la configuración de la herramienta, trabajando a través de ataques de Kali Linux y reenviando tráfico a sitios web específicos configurados de tal manera que no sean accesibles, configurar IDS e IPS.

CAPÍTULO IV: ESFUERZO PARA LA PERSONALIZACIÓN DE SURICATA

Análisis

Se realizará un análisis de cómo está estructurada la red interna de la empresa en donde se va a ejecutar la implementación de la herramienta de seguridad SURICATA, en la cual consiste en una revisión de los servidores de seguridad dado el caso de que los tenga y cuáles son las configuraciones actuales, caso contrario se realizará un análisis de cuáles son las vulnerabilidades que tiene la empresa y cuáles son los puertos permitidos para el debido funcionamiento de la red de la empresa, siendo estos los únicos que van a tener acceso y salida a la red externa que va a pasar por SURICATA.

Alcance: primera fase de pruebas

El alcance de mi implementación de la herramienta Suricata dentro de una red empresarial, podrá corregir las brechas de seguridad existentes y las futuras posibles que se presentarían dentro de la red de la empresa, en esta etapa se efectuará la primera fase de pruebas en la que se realizará Pentesting; validando así todas las vulnerabilidades que cuenta al momento la red empresarial en la cual se estará dando soporte, dado el caso de que sea una vulnerabilidad por Ingeniería Social; de la misma manera, se aplicará las pruebas al personal no técnico de la empresa.

Cálculo hora especializada

En esta etapa se realizará las fases de un test de penetración que consiste en 7 partes, y se detalla en horas laborables lo que toma cada una de estas y que se hace en las mismas.

- **Contacto:** Llega a un acuerdo entre partes en que va a consistir el test de penetración y acordar por escrito cual es el alcance del test (rango de la red, servicios o dispositivos). 4 horas.
- **Recolección de información:** Obtención de toda la información posible de la empresa, mediante escáneres de puerto en la red; para tener una idea de los sistemas y programas actuales como la calidad de los empleados (técnicos y no técnicos). 4-16 horas.
- **Modelado de amenaza:** En esta fase es indispensable pensar como atacante y utilizar toda la información recabada en el paso anterior y definir cuál va a ser la estrategia de penetración. 8 horas.
- **Análisis de vulnerabilidades:** Es prioridad valorar el posible éxito de la estrategia tomada para una penetración a la red exitosa, mediante la identificación proactiva de las vulnerabilidades, demostrando la habilidad y la creatividad para determinar y utilizar correctamente las herramientas para la fase de explotación. 8 horas.
- **Explotación:** En esta fase se intenta conseguir la penetración y explotación de las vulnerabilidades encontradas en los pasos anteriores, poniendo en práctica todo el conocimiento que se tenga para conseguir una penetración exitosa. 4-24 horas.
- **Post-explotación:** Una vez alcanzado el sistema del cliente, se comienza la fase en la cual se demostrará los daños y perdidas que podría suponer dicha brecha de seguridad para el cliente y la empresa. 4-24 horas.

- **Informe:** Finalmente se realizará el informe que se presentará al cliente con los resultados obtenidos de la auditoría aplicada a la red corporativa. 8-16 horas

Documentación

En la etapa de documentación se asumirá, que tipo de información se va a entregar al cliente ya sean estos: los manuales de instalación, manual de uso, manual de políticas de seguridad, acta entrega y recepción de lo documentación.

Para elaborar una constancia de todas las actividades realizadas en el punto anterior se completará toda la documentación anteriormente descrita y se detallará todas las anomalías encontradas, lo realizado y que documentación se quedará con el cliente.

Cálculo de presupuesto

El cálculo del presupuesto consiste en la sumatoria total de todas las horas invertidas en el proyecto siendo estas valoradas en un coste desde los $50, $70 y $100 hora especializada, de tal manera que se va a tener un valor diferente para cada tipo de empresa ya sean estas pequeñas, medianas y grandes empresas. A continuación, se detallará los posibles valores que tendrían en cada uno de los casos.

Tabla 5:

Tabla de los diferentes tipos de empresas.

TIPO	DEFINICIÓN	EMPLEADOS	CAPITAL
Pequeña Empresa	Se comprende a todas las empresas que no superan los 50 trabajadores.	0-50	No es superior a los 10 millones de dólares
Mediana Empresa	Se comprende a todas las empresas que tiene un rango	51-250	Hasta 43 millones de dólares

	de trabajadores entre 50 y 250.		
Gran Empresa	Se comprende a todas las empresas que superan los 250 trabajadores.	250++	Superior a 50 millones de dólares

Tipos de clientes:

Empresa pequeña

Tomando en cuenta la hora especializada a un coste de $50, para una empresa pequeña. Los siguientes datos a calcular son:

- Test de penetración: 40 horas.
- Implementación de la herramienta de seguridad: 24 horas.
- Documentación: 8 horas.

Dando un total estimado de 72 horas laborables con un coste total de $3.600.

Empresa mediana

Tomando en cuenta la hora especializada a un coste de $70, para una empresa mediana. Los siguientes datos a calcular son:

- Test de penetración: 68 horas.
- Implementación de la herramienta de seguridad: 24 horas.
- Documentación: 16 horas.

Dando un total estimado de 108 horas laborables con un coste total de $7.560.

Empresa grande

Tomando en cuenta la hora especializada a un coste de $100, para una empresa grande. Los siguientes datos a calcular son:

- Test de penetración: 100 horas.

- Implementación de la herramienta de seguridad: 24 horas.
- Documentación: 16 horas.

Dando un total estimado de 140 horas laborables con un coste total de $14.000.

Síntesis del capítulo

Este capítulo analiza la parte real del proyecto y el trabajo de desarrollo que se realizará, junto con los costos que se aplicará a cada una de estas fases.

CONCLUSIONES

- Luego de analizar la teoría y los conceptos relacionados con el tema de ciberseguridad en Ecuador, se concluye que es importante conocer las leyes y regulaciones que rigen este tema para garantizar la protección de la información y los derechos de los usuarios en el entorno digital. Además, es fundamental tener en cuenta la evolución histórica de la ciberseguridad para comprender la importancia de este tema en la sociedad actual y las implicaciones que tiene en la vida cotidiana. En conclusión, la ciberseguridad es un aspecto fundamental para garantizar la privacidad y seguridad en el entorno digital y es necesario tomar medidas para proteger la información y los derechos de los usuarios en línea.
- Posterior al análisis de la parte estadística y analítica, se concluye que los resultados muestran una tendencia hacia una falta de conciencia en cuanto a la ciberseguridad en el entorno empresarial. Los datos indican que las personas encargadas dentro de las empresas tienen una baja comprensión de las vulnerabilidades y los riesgos en el entorno digital. Esto indica la necesidad de implementar medidas de concientización y capacitación en ciberseguridad para garantizar la protección de la información y los activos digitales de las empresas. En conclusión, la ciberseguridad es un aspecto crítico en el entorno empresarial y es necesario tomar medidas para mejorar la conciencia y la preparación ante los riesgos en el entorno digital.
- Después de cubrir la parte práctica del proyecto y la configuración de las herramientas, se concluye que la implementación de sistemas de detección y prevención de intrusiones (IDS e IPS) puede ser efectiva en la protección

de los sistemas y redes contra ataques externos. La realización de ataques a través de Kali Linux y el reenvío de tráfico a sitios web específicos demuestra la importancia de estar preparado ante posibles amenazas y la necesidad de implementar medidas de seguridad para prevenir y mitigar los impactos de un ataque. En conclusión, la configuración e implementación de sistemas de seguridad cibernética es un aspecto clave en la protección de los activos digitales y es necesario mantenerlos actualizados y monitoreados para garantizar la seguridad en el entorno digital.

- En el análisis de la parte real del proyecto y el trabajo de desarrollo que se realizará, se concluye que la implementación de un proyecto de seguridad cibernética es un proceso costoso que requiere una planificación cuidadosa y una evaluación constante de los costos. Es importante tener en cuenta los costos asociados con cada fase del proyecto y asegurarse de que estos se encuentren dentro del presupuesto disponible. En conclusión, la gestión adecuada de los costos es fundamental para garantizar el éxito de un proyecto de seguridad cibernética y es necesario considerar cuidadosamente todas las implicaciones financieras antes de comenzar el proyecto.

RECOMENDACIONES

Suricata es recomendable para empresas las cuales se están creando como para las empresas que ya tienen una trayectoria a nivel país o internacional, SURICATA es un complemento para la seguridad de la red empresarial, pues brinda una ayuda tanto para pequeñas empresas como son las configuraciones básicas o predeterminadas por la herramienta de protección de red SURICATA como para las empresas grandes en las cuales se realizará una configuración mucho más personalizada implementando y creando las propias reglas las cuales se adaptan a la empresa requirente siendo así un soporte más para la protección y cuidado de los activos y bienes empresariales.

Independientemente del tamaño de la empresa, implementar esta herramienta será de utilidad para los responsables de la ciberseguridad, la cual permite tener un control más detallado y minucioso de lo que está sucediendo dentro de la red.

REFERENCIAS BIBLIOGRÁFICAS

Alvarado Chang, J. E. (2 de Mayo de 2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *Revista Científica Aristas*, 25. doi:ISSN: 2600-5662

Arias, E. R. (2022, November 24). Investigación exploratoria. Economipedia. https://economipedia.com/definiciones/investigacion-exploratoria.html

Arcotel. (2018). *Resolución Arcotel-2018-0652.* Arcotel. Quito: Agencia de Regulación y Control de las Telecomunicaciones. Recuperado el 3 de Agosto de 2022, de https://www.gob.ec/sites/default/files/regulations/2018-10/ARCOTEL-2018-0652-2018-07-31-TELECOMUNICACIONES-MATRIZ.pdf

Bokmal, N., Güelfo, J., & Encripto AS - Information. (4 de Mayo de 2022). *Encripto AS - Information Security*. Obtenido de Network Security Monitoring – What is it all about?: https://www.encripto.no/2016/09/network-security-monitoring-2/

Check Point ThreatCloud. (4 de Agosto de 2022). *Live Cyber Threat Map*. Obtenido de Check Point ThreatCloud: https://threatmap.checkpoint.com/

Ciberseg1922. (19 de Mayo de 2021). *Qué es el Marco MITRE ATT&CK y cómo implementarlo*. Obtenido de Ciberseguridad: https://ciberseguridad.com/herramientas/marco-mitre-att-ck/

CISCO. (17 de Febrero de 2022). *CISCO*. Obtenido de Introduction to Cybersecurity: https://contenthub.netacad.com/legacy/I2CS/2.1/es/index.html#1.1.1.1

CISCO. (17 de Febrero de 2022). *CISCO*. Obtenido de Introduction to Cybersecurity: https://contenthub.netacad.com/legacy/I2CS/2.1/es/index.html#2.1.1.1

COIP. (2021). Código Orgánico Integral Penal. *Oficio No. SAN-2014-0138* (págs. 68,75, 90). Quito: COIP. Recuperado el 3 de Agosto de 2022, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Cuarta Sesión Plenaria OEA. (2004). ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA:

UN ENFOQUE MULTIDIMENSIONAL Y MULTIDICIPLIANRIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA. *AG/RES. 2004 (XXXIV-O/04)* (págs. 2, 3). Montevideo: OEA. Recuperado el 3 de Agosto de 2022, de https://www.oas.org/es/sms/cicte/documents/asambleas/ag-res.%202004%20(xxxiv-o-04)_sp.pdf

EC-Council. (28 de Junio de 2019). *10 Errores de Seguridad Que Todas las Pequeñas Empresas deben Evitar*. Obtenido de ETIC Solutions S.A.S: https://etic-solutions.net/etic/10-errores-de-seguridad-que-todas-las-pequenas-empresas-deben-evitar

Fortinet. (4 de Agosto de 2022). *Threat Analytics Ecuador*. Obtenido de FortiGuard Labs: https://www.fortiguard.com/threat-research/map/country/EC

Güelfo, J. J. (2022, May 4). Network Security Monitoring (NSM) and what it is all about - Encripto AS. Encripto AS - Information Security. https://www.encripto.no/2016/09/network-security-monitoring-2/

INCIBE. (7 de Abril de 2017). *La seguridad vista desde sus inicios*. Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

INCIBE. (30 de sEPTIEMBRE de 2020). *¿Qué son y para qué sirven los SIEM, IDS e IPS?*|. Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

Lara Guijarro, E. G. (2019). *DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN OSSTMMv3, NIST SP 800-30 E ISO 27001, PARA CENTROS DE EDUCACIÓN: CASO DE ESTUDIO UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES, EXTENSIÓN TULCÁN*. Universidad Internacional SEK, FACULTAD DE ARQUITECTURA E INGENIERÍAS. Tulcan: Universidad Internacional SEK. Recuperado el 10 de Diciembre de 2021, de https://repositorio.uisek.edu.ec/bitstream/123456789/3260/1/TESIS%20ELVA%20LARA.pdf

Ley Organica de Telecomunicaciones. (2015). Ley Organica de Telecomunicaciones. *Oficio No. SAN-2015-0263* (pág. 22). Quito: Nacional.

Logística Actualizada (Dirección). (2014). *¿Qué son las PYMEs?* [Película]. Mexico. Recuperado el 11 de Agosto de 2020, de https://www.youtube.com/watch?v=itk1uRAEntU

Malwarebytes. (25 de Noviembre de 2019). *Ransomware: qué es y cómo eliminarlo.* Obtenido de Malwarebytes.com: https://es.malwarebytes.com/ransomware/

Microsoft Security Response Center. (29 de Noviembre de 2017). *Microsoft MSRC*. Obtenido de Vulnerabilities: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11882

Network Working Group. (Enero de 1993). *Internet Users' Glossary.* Obtenido de RFC 1392: https://dl.acm.org/doi/pdf/10.17487/RFC1392

Network Working Group. (Enero de 1993). *Internet Users' Glossary.* Obtenido de RFC 1392: https://dl.acm.org/doi/pdf/10.17487/RFC1392

OEA; BID; Centro Global de Capacidad en Seguridad Cibernética, Universidad de Oxford . (2020). *CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE* . Obtenido de IBD: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Ortiz, D. (03 de Septiembre de 2021). *El Comercio.* Obtenido de Los ataques informáticos a pymes crecen en el Ecuador: https://www.elcomercio.com/tendencias/tecnologia/ataques-informaticos-pymes-crecen-ecuador.html

Solutions, E. (2019, June 28). 10 Errores de Seguridad Que Todas las Pequeñas Empresas deben Evitar. ETIC Solutions S.A.S. https://etic-solutions.net/etic/10-errores-de-seguridad-que-todas-las-pequenas-empresas-deben-evitar

Shabi, T., Hasson, E., Gravier, O., Avital, N., Lowing, S., & Lynch, B. (29 de Diciembre de 2019). *Advanced persistent threat (APT)*. Obtenido de

Imperva: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

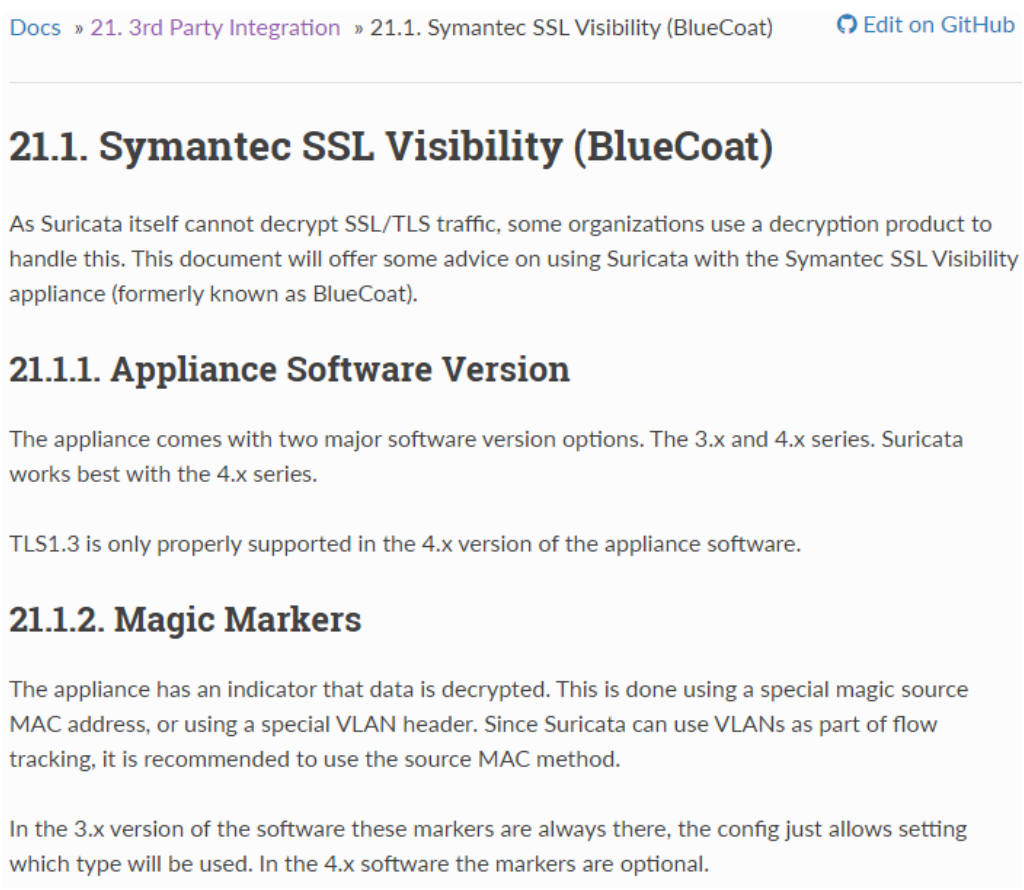
Torres, A. E. (10 de Junio de 2021). *Network Traffic Analysis: ¿Qué es un archivo PCAP?* Obtenido de Linkedin: https://www.linkedin.com/pulse/network-traffic-analysis-qu%C3%A9-es-un-archivo-pcap-arturo-e-torres/?originalSubdomain=es

ANEXOS

Figura 71:
Que es Suricata.

Fuente: (OISF Revision bf1c185c., 2022c)

Figura 72:
Integración con terceros.



Docs » 21. 3rd Party Integration » 21.1. Symantec SSL Visibility (BlueCoat) Edit on GitHub

21.1. Symantec SSL Visibility (BlueCoat)

As Suricata itself cannot decrypt SSL/TLS traffic, some organizations use a decryption product to handle this. This document will offer some advice on using Suricata with the Symantec SSL Visibility appliance (formerly known as BlueCoat).

21.1.1. Appliance Software Version

The appliance comes with two major software version options. The 3.x and 4.x series. Suricata works best with the 4.x series.

TLS1.3 is only properly supported in the 4.x version of the appliance software.

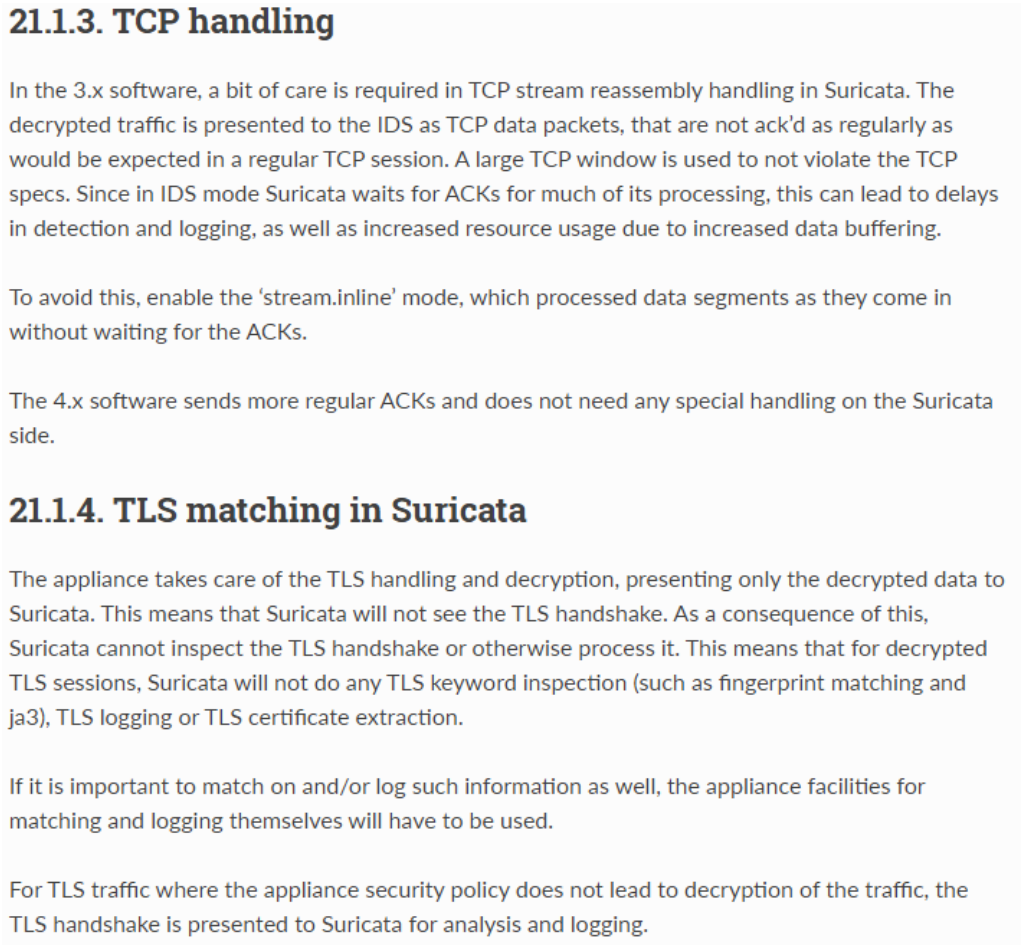
21.1.2. Magic Markers

The appliance has an indicator that data is decrypted. This is done using a special magic source MAC address, or using a special VLAN header. Since Suricata can use VLANs as part of flow tracking, it is recommended to use the source MAC method.

In the 3.x version of the software these markers are always there, the config just allows setting which type will be used. In the 4.x software the markers are optional.

Fuente: (OISF Revision bf1c185c., 2022b)

Figura 72.1:
Integración con terceros.



21.1.3. TCP handling

In the 3.x software, a bit of care is required in TCP stream reassembly handling in Suricata. The decrypted traffic is presented to the IDS as TCP data packets, that are not ack'd as regularly as would be expected in a regular TCP session. A large TCP window is used to not violate the TCP specs. Since in IDS mode Suricata waits for ACKs for much of its processing, this can lead to delays in detection and logging, as well as increased resource usage due to increased data buffering.

To avoid this, enable the 'stream.inline' mode, which processed data segments as they come in without waiting for the ACKs.

The 4.x software sends more regular ACKs and does not need any special handling on the Suricata side.

21.1.4. TLS matching in Suricata

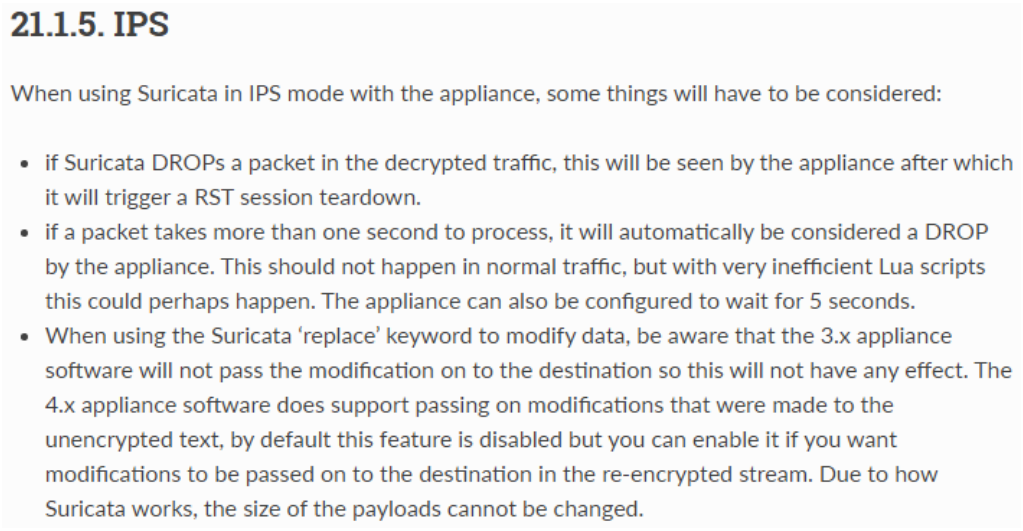
The appliance takes care of the TLS handling and decryption, presenting only the decrypted data to Suricata. This means that Suricata will not see the TLS handshake. As a consequence of this, Suricata cannot inspect the TLS handshake or otherwise process it. This means that for decrypted TLS sessions, Suricata will not do any TLS keyword inspection (such as fingerprint matching and ja3), TLS logging or TLS certificate extraction.

If it is important to match on and/or log such information as well, the appliance facilities for matching and logging themselves will have to be used.

For TLS traffic where the appliance security policy does not lead to decryption of the traffic, the TLS handshake is presented to Suricata for analysis and logging.

Fuente:(OISF Revision bf1c185c., 2022b)

Figura 72.2:
Integración con terceros.



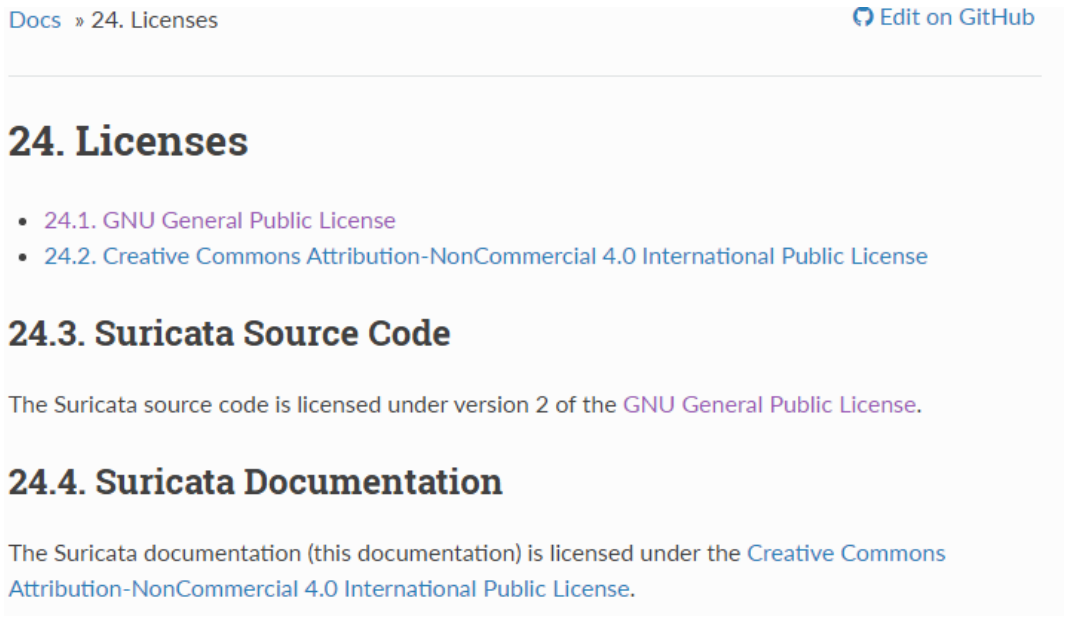
21.1.5. IPS

When using Suricata in IPS mode with the appliance, some things will have to be considered:

- if Suricata DROPs a packet in the decrypted traffic, this will be seen by the appliance after which it will trigger a RST session teardown.
- if a packet takes more than one second to process, it will automatically be considered a DROP by the appliance. This should not happen in normal traffic, but with very inefficient Lua scripts this could perhaps happen. The appliance can also be configured to wait for 5 seconds.
- When using the Suricata 'replace' keyword to modify data, be aware that the 3.x appliance software will not pass the modification on to the destination so this will not have any effect. The 4.x appliance software does support passing on modifications that were made to the unencrypted text, by default this feature is disabled but you can enable it if you want modifications to be passed on to the destination in the re-encrypted stream. Due to how Suricata works, the size of the payloads cannot be changed.

Fuente: (OISF Revision bf1c185c., 2022b)

Figura 73:
Licencias.



Fuente: (OISF Revision bf1c185c., 2022a)