ANÁLISIS Y GESTIÓN DEL COMPORTAMIENTO DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON DISPOSITIVOS DE BAJO COSTO PYMES EN BOGOTÁ Y ALREDEDORES

RICHARD GIL BARRETO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

ANÁLISIS Y GESTIÓN DEL COMPORTAMIENTO DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON DISPOSITIVOS DE BAJO COSTO PYMES EN BOGOTÁ Y ALREDEDORES

RICHARD GIL BARRETO

Proyecto de Grado – Investigación presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Director
Alexander Larrahondo
Tutor de Curso
Edgar Mauricio López

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a todos aquellos que han sido influencia positiva en mi vida cuya compresión y apoyo generan la combustión para seguir adelante en esta nueva etapa, a mi esposa que me impulsa a seguir cultivando frutos y especial a su paciencia silenciosa durante este momento de desarrollo de estas actividades.

AGRADECIMIENTOS

Agradezco al universo por poner en nuestro camino a los maestros y ángeles que nos orientan durante el camino que elegimos, a mi familia y esposa que nos impulsan a crecer personal y profesionalmente cada día más y a las directivas de la Universidad Nacional Abierta y a Distancia UNAD.

CONTENIDO

pág.

INTRODUCCIÓN *13*

1. DEFINICIÓN DEL PROBLEMA *14*

1.1 ANTECEDENTES DEL PROBLEMA 14

1.2 FORMULACIÓN DEL PROBLEMA 14

1.3 PLANTEAMIENTO 15

2 JUSTIFICACIÓN *16*

3 OBJETIVOS *17*

3.1 OBJETIVOS GENERAL 17

3.2 OBJETIVOS ESPECÍFICOS 17

4 MARCO REFERENCIAL *18*

4.1 MARCO TEÓRICO 18

4.1.1. Contra medidas. 19

4.1.2. Seguridad informática en redes. 21

4.1.3. Software código libre. 22

4.1.4. IDS y su clasificación. 22

4.1.5. Requisitos de un IDS. 22

4.1.6. Características. 23

4.1.7. Taxonomía reglas en un IDS. 23

4.2 MARCO CONCEPTUAL 25

5 EVALUACIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS IDS DE CÓDIGO ABIERTO *26*

5.1 SURICATA 26

5.2 SNORT 27

5.3 COMPARATIVO CARACTERISTICAS 28

6 PRUEBAS IDS IDENTIFICANDO EL GRADO DE DIFICULTAD DURANTE SU IMPLEMENTACIÓN *29*

6.1 REQUISITOS PARA LA IMPLEMENTACIÓN DE UN IDS – SURICATA 29

6.2 REQUISITOS PARA LA IMPLEMENTACIÓN DE UN IDS – SNORT 30

6.3 SINGLE BOARD 33

6.4 EVALUACION IDS 35

6.4.1 Variable Funciones.....35
6.4.2 Variable desempeño.....36
6.4.3 Variable Seguridad.....36

7 PROCEDIMIENTO DE IMPLEMENTACIÓN DE UN IDS DE CÓDIGO ABIERTO - GUIA PARA LAS PYMES ***37***

8 RECOMENDACIONES ***42***

9 CONCLUSIONES ***45***

10 ANEXOS ***46***

11 BIBLIOGRAFÍA ***47***

LISTA DE FIGURAS

	Pag.
Figura 1. Diagrama esquemático de un IDS	21
Figura 2. Componentes de una regla en un IDS	23
Figura 3. Taxonomía regla IDS	24
Figura 4. Ejemplo regla IDS	24
Figura 5. Suricata versión y características	30
Figura 6. Topología de red en una Pyme	32
Figura 7. Flujo motor de detección	33
Figura 8. Raspberry pi	34
Figura 9: Cargando el SO Debian en MicroSD	37
Figura 10: Regla personalizada monitoreo ICMP	40
Figura 11: Alerta detectada por el IDS	40
Figura 12: Alerta detectada por el IDS por escaneo de vulnerabilidades	41
Figura 13: Alerta detectada por el IDS al acceder los DNS .onion	41
Figura 14: Alerta detectada por el IDS al intentar descargar un archivo con virus	41

LISTA DE TABLAS

	Pag.
Tabla 1. Evaluación sistemas de detección de intrusos – IDS	29
Tabla 2. Comparativo de características IDS	31
Tabla 3. Valoración indicador de funciones	35
Tabla 4. Valoración indicador de desempeño	36
Tabla 5. Valoración indicador seguridad	36

GLOSARIO

AMENAZA: Evento que puede generar daño a un sistema

FIREWALL: Herramienta de seguridad perimetral que permite el control del tráfico entrante y saliente de las peticiones de comunicación entre redes.

IDS: Sistema de detección de intrusos, realiza la detección de comportamientos anómalos dentro de la red.

IP: Protocolo de internet que hace parte de la capa de red permitiendo el transporte de paquetes.

IPS: Sistema de prevención de intrusos, es un hardware o software que provee seguridad durante en análisis del tráfico de red en busca de patrones de ataques para denegarlos.

PROTOCOLO: Reglas por las que se rigen el intercambio de datos en una red

SOFTWARE LIBRE: Aplicaciones desarrolladas para su uso y distribución mediante la licencia GPL.

VLAN: Es una red de área local virtual, método para crear redes de manera lógica dentro de una infraestructura de red física.

RESUMEN

El presente documento plantea la necesidad de analizar el funcionamiento, rendimiento, comportamiento ante incidentes de seguridad de los sistemas de detección de intrusos IDS y de los Sistemas de Protección contra Intrusos IPS en la protección de las infraestructuras tecnológicas de las pymes. Apoyando al proyecto de investigación denominado: “Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD”. Aportando a este proyecto institucional “Centro de Innovación y Productividad – CIP CSIRT Académico UNAD” con información relevante de la seguridad informática y los diferentes incidentes que sufren las pymes.

ABSTRACT

This document raises the need to analyze the operation, performance, behavior in the face of security incidents of intrusion detection systems IDS and Intrusion Protection Systems IPS in the protection of technological infrastructures of SMEs. Supporting the research project called: "Proposal for the Creation and Consolidation of the Computer Incident Response Center of the National Open and Distance University CSIRT-UNAD". Contributing to this institutional project "Center for Innovation and Productivity - CIP CSIRT Academic UNAD" with relevant information on computer security and the different incidents suffered by SMEs.

INTRODUCCIÓN

Existen una gran complejidad al momento de tomar la determinación de crear una infraestructura de datos o redes cableadas, hay un sin número de posibilidades de crear estas redes junto con equipos, servidores, routers, switches, firewall, appliance que aportan gran valor a cada organización independiente su naturaleza.

Los centros de datos buscan tener redundancia en sus operaciones y en sus puntos más críticos que afectan la operación de la organización, minimizando el riesgo. Sin embargo, esto no es suficiente para poder decir que tenemos un control optimo que permita evitar las amenazas de los ciberdelincuentes.

Hay varias alternativas que permiten robustecer estas redes de comunicaciones mediante hardware y software, pero su uso y aplicabilidad no es sencillo al momento de entrar a operar estas soluciones. Para las empresas estos cambios e implementaciones genera un impacto debido a sus elevados costos y los tiempos de puesta en marcha, sumando las horas ingeniero necesarias para el afinamiento de estas herramientas.

Para las Pymes es aún un mayor riesgo siendo una gran cantidad de empresas en el país, sumando que no cuentan actualmente con los recursos necesarios para inversiones en tecnología que abarque soluciones de tipo IDS/IPS.

Es así como encontramos software libre que reduce sustancialmente la implementación de estas soluciones informáticas y si proveen de una gran visibilidad dentro de lo ocurrido en las redes de comunicaciones tanto internas como externas.

Habrá que invertir tiempo y esfuerzos necesarios con los conocimientos afianzados para una óptima implementación de soluciones tipo IDS dentro de una organización.

La posibilidad de restringir aquellas comunicaciones que son fraudulentas o no autorizadas, el denegar aquellos servicios que no deben de estar habilitados desde ciertas ip de de origen especificadas, el bloqueo de paquetes que viajan en la red con virus o posibles amenazas que pueden afectar la operación continua con los aspectos que trataremos más adelante.

Tener la visual de como una red debe operar usando los diversos protocolos se generarán patrones de comportamiento que luego será posible analizar y generar reglas para cada uno de ellos mediante el uso de los IDS y las firmas de amenazas posibles.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Según Kaspersky en su informe anual reveló que en el 2021 en América latina aumentaron los ciberataques en un 24% durante los primeros 8 meses del año, donde toma los 20 programas maliciosos comúnmente más usados, representando más de 728 millones de incidentes de seguridad más o menos 35 ataques por segundo y si nos centramos en Colombia alrededor de 85 ataques por segundo.

Según el informe de Tendencias del Cibercrimen en Colombia (2019-2020) la mayoría de las pymes en Colombia luego de ser víctimas de los ciberdelincuentes no pueden mantener sus negocios y se van a la quiebra o bancarrota no quedando más que cerrar su operación. Esto es debido a que dentro del corto presupuesto si es que lo tienen no cuentan con sistemas robustos de ciberseguridad, lo que las hace el blanco preferido de los ciberdelincuentes y al tener negocios con otras empresas de mayor operación son usadas como puente para alcanzar sus infraestructuras tecnológicas y su información.

Para las Pymes la seguridad informática está teniendo un mayor protagonismo para integrarlos dentro de sus infraestructuras, permitiendo mediante el uso de nuevas tecnologías y herramientas de monitoreo tener visibilidad de los ataques cibernéticos y posibles amenazas, permitiendo tomar acciones de manera inmediata evitando las fugas o pedida de información.

La operación continua de una infraestructura es respaldada por estos sistemas de monitoreo generando los datos necesarios para tomar las remediaciones y mitigaciones adecuadas para no afectar el plan estratégico de las mismas, brindando seguridad y estabilidad a los clientes internos y externos.

1.2 FORMULACIÓN DEL PROBLEMA

Las Pymes en su gran mayoría no cuentan en su departamento de TI o no contemplan dentro de un Plan de Seguridad la adopción de soluciones como las de IDS/IPS existentes en el mercado precisamente por los costos tan elevados.

Actualmente hay alternativas que permiten tener un entorno más seguro, surgen soluciones de código libre que cubren esta necesidad brindando la posibilidad de control dentro de su infraestructura.

1.3 PLANTEAMIENTO

Para las empresas hoy en día están empleando la adopción de políticas como BYOD (Bring Your Own Device), permitiendo que los empleados usen sus diferentes dispositivos como portátiles, móviles, tabletas, etc. Implica esta tendencia retos de seguridad que entre otros permitan blindar los datos sensibles y accesos a las redes, así como un aumento en los riesgos a los que se exponen la empresa al no controlar, monitorear y gestionar estos dispositivos.

Es en este escenario donde los IDS pueden jugar un papel importante para ayudar a realizar los controles y monitoreos de las redes en donde estos equipos se conectan, como es difícil implementar controles sobre los equipos personales si es posible hacerlo monitoreando el tráfico de la red.

Este análisis de los IDS permite detectar y/o analizar los comportamientos anómalos y a las posibles amenazas que pueden afectar la infraestructura, es acá donde se realiza la integración de software de código libre bajo un licenciamiento open source.

2 JUSTIFICACIÓN

Los ciberdelincuentes están usando empresas pymes como puente para generar ataques cibernéticos a otras organizaciones de diferentes países, y muchas de las organizaciones no cuentan con la posibilidad de tener mecanismos automáticos para evitar o identificar cuando esto ocurre al interior de las empresas.

Evitar ser víctima de los ciberdelincuentes mediante los sistemas de detección y prevención de intrusos, logrando tomar acciones tanto preventivas como correctivas dentro de la infraestructura de las pymes.

Con la gestión y detección de intrusos dentro de la infraestructura de las pymes es posible generar reglas y remediaciones para evitar la propagación del ataque informático, minimizando la pérdida o fuga de información.

Los sistemas de prevención y detección de intrusos realizan un análisis del tráfico de la red, reportes de posibles vectores de ataque, comportamientos anómalos, clasificación de las amenazas, control de vulnerabilidades generando una mayor información del comportamiento de la infraestructura actual permitiendo mitigar, restringir o denegar y tomar acciones cuando algún evento este generando afectación sobre dicha infraestructura.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Análisis de los diferentes sistemas de detección de intrusos de código libre, validando las características, funcionalidades como aporte a la investigación del proyecto de Análisis del comportamiento de un IDS implementado en equipos de bajo costo en pymes para el semillero de ceros y unos.

3.2 OBJETIVOS ESPECÍFICOS

Evaluar los sistemas de detección de intrusos IDS de código abierto existentes en el mercado permitiendo identificar las mejores opciones a trabajar dentro del proyecto de investigación.

Desarrollar pruebas con los IDS mejor evaluados permitiendo identificar las curvas de aprendizaje y grado de dificultad en su implementación.

Realizar un procedimiento de implementación de un IDS de código abierto como guía para las Pymes.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Dentro del mundo tecnológico existen una gran variedad de posibilidades que permiten la identificación de “Sistemas de Detección de Intrusos en una Red” [1] cual sistema de IDS puede llegar a ser el más adecuado en términos de costo efectivo, y es allí donde surge la necesidad de buscar la mejor alternativa en dispositivos donde sea posible realizar la implementación de este tipo de soluciones mediante el uso del software libre.

La manera de proteger los activos y los sistemas de información está emergiendo con las grandes empresas que generan productos y equipos que integran soluciones de IDS y soluciones IPS, estas plataformas y equipos terminan con costos elevados donde se suman a estos valores las licencias, costos de uso de tráfico entre otros. Es así como “actualmente existen multitud de herramientas de código abierto para la detección y prevención de intrusos” [2] que pueden ser configurables en equipos con requerimientos mínimos, permitiendo que estas soluciones sean tenidas en cuenta por los equipos de TI, por el CSO, por los equipos de gobernanza de TI y en el caso de las Pymes también deberían ser consideradas.

Los IDS/IPS tienen una gran ventaja para las Pymes y es precisamente su granularidad y configuración personalizada para cada entorno, facilitando generarlos escenarios adecuados para generar las reglas y políticas dentro de cada pyme autorizando o denegando todo aquello que es permitido.

Una organización con los recursos suficientes podrá realizar la adquisición de soluciones IDS / IPS de marcas como CISCO, IMPERVA, SonicWall, Radware, sin embargo, no todas las Pymes cuenta con los recursos necesarios para la adquisición de soluciones de dichas marcas. Mediante el uso de soluciones de código abierto es posible que las Pymes puedan tener dentro de su estructura una solución tipo IDS/IPS que brinde mayor seguridad a los diferentes sistemas de información y mantener una infraestructura segura. Adicional encontramos un artículo llamado “Implementing an Intrusion Detection and Prevention System Using Software-Defined Networking: Defending Against Port-Scanning and Denialof-

[1] Solarte, Ocampo, Bermúdez, Sistema de detección de intrusos en redes corporativas. Scientia et Technica.2017, p.3

[2] Soucase Iranzo. Implementación de un Sistema de Prevención de Intrusiones (IPS) en un modelo de red industrial. 2021. p24

Service Attacks"[3]. Permitiendo tener una idea de los aspectos más importantes al momento de realizar una configuración de un IDS para una red.

Durante los años 2019 y 2020 el tercer delito informático en Colombia más reportado es el acceso abusivo a sistema informático con 7.994, es así como in IDS /IPS busca proteger el acceso no autorizado a los diferentes sistemas de información como bases de datos entre otros.

Dentro de las necesidades actuales en las organizaciones encontramos de manera fundamental tener un sistema de detección de intrusos dentro de la red permitiendo frente a las ciber amenazas tener una herramienta que identifique las anomalías frente a los sistemas de información críticos que se desea proteger.

Adicional es importante contar con los activos que se desean blindar o proteger para aplicar las reglas, políticas, alertas y configuraciones necesarias son la implementación de un IDS.

Esta parametrización, personalización, integración, configuración e implementación es posible realizarla mediante software de código libre Kernel GNU/Linux y puede ser usada por las Pymes.

4.1.1. Contra medidas. Una infraestructura tecnología cuenta con diversos equipos de red, servidores y appliance que regularmente tienen una función particular dentro de cada organización, existen por ejemplo aquellos equipos encargados de la administración de las redes de comunicación como los switches y routers.

Estos equipos cuentan con algunos parámetros de configuración que pueden ayudar a regular los controles y accesos a nivel de red, usando medidas como VLAN, ACL, rutas y protocolos de enrutamiento.

Otro equipo para mencionar son los Firewall mediante estos equipos pueden generarse una gran cantidad de configuraciones a nivel de red. Proveen la capacidad de denegar o permitir los flujos de tráfico requeridos según las políticas aplicadas, pero en su mayoría no cuentan con una solución IDS/IPS que permita realizar todo el análisis de la red identificando los posibles tráficos de red que pueden o no ser permitidos, así como los paquetes maliciosos que viajan por la red.

Existen varias razones por las cuales una pequeña o mediana empresa (Pyme) podría considerar la implementación de una solución IDS (Sistema de Detección de Intrusos).

[3] Birkinshaw C, Rouka E, Vassilakis VG. Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. Journal of Network and Computer Applications. 2019

Presupuesto Limitado: Las Pymes a menudo tienen recursos financieros limitados para dedicar a la seguridad cibernética. Utilizar dispositivos de bajo costo puede ser una forma más asequible de mejorar la seguridad de la red en comparación con soluciones más costosas.

Protección de Activos Críticos: Aunque una Pyme pueda ser pequeña en tamaño, puede poseer activos digitales críticos, como datos de clientes, propiedad intelectual o información financiera. La implementación de un IDS ayuda a proteger estos activos de posibles amenazas.

Cumplimiento Normativo: En muchos casos, las Pymes también deben cumplir con regulaciones y estándares de seguridad cibernética. Un IDS puede ayudar a cumplir con estos requisitos y evitar posibles sanciones.

Detección Temprana de Amenazas: Un IDS eficaz puede detectar intrusiones y amenazas en tiempo real o casi en tiempo real. Esto permite a la Pyme tomar medidas inmediatas para mitigar cualquier amenaza antes de que cause un daño significativo.

Minimización de Falsos Positivos: Los dispositivos de bajo costo a menudo se pueden configurar de manera más personalizada para reducir los falsos positivos, lo que significa que la Pyme no está inundada de alertas innecesarias.

Escalabilidad: A medida que la Pyme crece, puede escalar su infraestructura de seguridad y puede implementar dispositivos de bajo costo o aumentar la cantidad de dispositivos de bajo costo para tener una solución más robusta en diversas zonas de la red.

Flexibilidad: Las soluciones de software libre y dispositivos de bajo costo a menudo son flexibles y pueden adaptarse a las necesidades específicas de la Pyme. Esto permite una personalización más eficiente frente a otras soluciones del mercado

Comunidad de Soporte: Muchas soluciones de software libre cuentan con comunidades activas de usuarios y desarrolladores que pueden proporcionar soporte y recursos de forma gratuita o a un costo menor en comparación con soluciones propietarias.

Concienciación de la Seguridad: La implementación de un IDS puede fomentar la concientización de la seguridad cibernética dentro de la Pyme, lo que puede llevar a prácticas más seguras por parte de los empleados y reducir el riesgo de incidentes.

Evolución de las Amenazas: Las amenazas cibernéticas evolucionan constantemente y pueden afectar a empresas de todos los tamaños. Tener un IDS

en su lugar proporciona una capa adicional de protección contra amenazas emergentes.

La ubicación de un IDS se puede tener en diversos ámbitos y dependerá mucho de la estructura de red o infraestructura que se desee proteger, la figura 1 muestra un diagrama estándar de la ubicación de un IDS.

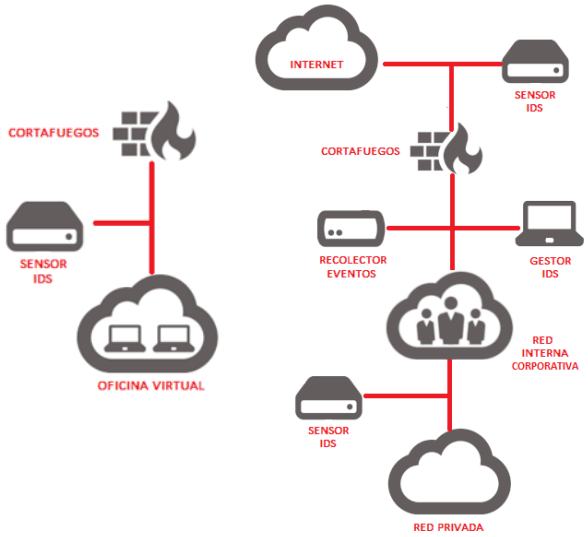


Figura 1. Diagrama esquemático de un IDS
Fuente: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

4.1.2. Seguridad informática en redes. Las pymes visualizan la seguridad informática más allá de una inversión como un gasto que no genera ningún aporte a los planes estratégicos, sin embargo, los IDS son supremamente útiles al momento de brindar seguridad en las redes de área local.

El diseño y puesta en marcha de los módulos necesarios para realizar el montaje correspondiente es complejo. La parametrización de una solución IDS varía según el escenario de cada Pyme ya que involucra una red completamente diferente en cada una de ellas.

Los archivos deben ajustarse de manera manual en cada uno de sus apartados aportando una granularidad sobre la red y en el tratamiento que debe aplicarse cuando ocurra alguna anomalía que alerte a los sistemas IDS. Podemos mencionar Snort como uno de los principales IDS usados en el mundo por grandes compañías.

Los sistemas de intrusión aportan dentro de la seguridad de la información a mantener la integridad, confidencialidad y disponibilidad de los recursos, adicional protegen los recursos dentro de la red de accesos no autorizados.

4.1.3. Software código libre. El uso de software de código libre o abierto abre una gran posibilidad para la implementación de un gran número de soluciones para la gran mayoría de entornos, dentro del licenciamiento existente para el uso de software libre la posibilidad de tener ciertas libertades como ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software.

4.1.4. IDS y su clasificación. Hoy en día los IDS los podríamos catalogar en grupos cuyas soluciones son enfocadas a la detección de intrusión encargados de realizar la vigilancia dentro de las redes o los otros enfocados en función de cómo hacen dicho proceso esto quiere decir que hay la posibilidad de realizar los análisis de redes dentro de una misma red o subredes.

IDS Basados en red indica el análisis de todo el tráfico de la red mediante la captura de los paquetes del dominio de colisión que transitan en la misma, puede realizarse en la red y no en un único host.

IDS Basados en host indica que solo se puede tener un equipo y su monitoreo se hace de manera exclusiva, actúa de manera similar a los escudos antivirus pero enfocado al tráfico de red.

4.1.5. Requisitos de un IDS. Sin importar qué sistemas vigile o su forma de trabajar, cualquier sistema de detección de intrusos ha de cumplir algunas propiedades para poder desarrollar su trabajo correctamente.

Dentro una implementación se debe tener en cuenta algunos aspectos importantes sobre un IDS debido a que se genera un impacto frente al uso de las redes y las comunicaciones existentes dentro de una empresa que desee realizar una inclusión de uno de estos sistemas de detección de intrusos.

Cuando se usan los IDS basados en host ocurrirá que la maquina estará analizando constantemente los paquetes de red y esto genera que se eleve el uso del procesamiento y memoria de esta. Cabe mencionar que este análisis será constante y se tomaran las acciones según como se hayan parametrizado, generando las alertas, logs correspondientes.

Para los IDS basados en red, el análisis será de todo el tráfico que circula en la red, donde se tomaran las muestras de todos los paquetes pudiendo generar falsos positivos que pueden ocasionar que los administradores de red tengan que nuevamente generar un afinamiento de los archivos previamente configurados.

En este punto es importante tener un conocimiento amplio de redes para que el afinamiento y configuraciones finales de un IDS se tengan en cuenta los valores de las direcciones ip de origen, destino, puertos, banderas del protocolo TCP, etc. Permitiendo que los vectores de ataque que se logren visualizar tengan la mayor información posible para tomar acciones cuando el evento ocurra.

4.1.6. Características. El flujo de tráfico dentro de la red permite generar diferentes patrones de comportamiento los cuales corresponde a diferentes actividades que se encuentran dentro de las firmas que tiene un IDS. Este análisis de las firmas permite identificar dentro de la red los paquetes que son catalogados como sospechosos donde algunos casos pueden ser falsos positivos y se deben de ajustar según corresponda.

Los IDS tienen varias características que generan un gran valor para las empresas u organizaciones independientes de su naturaleza que implementan este tipo de soluciones en su infra estructura como, por ejemplo:

- Capacidad de reacción ante un ataque
- Durante un ataque se pueden aplicar nuevos filtros
- No requiere supervisión
- Generación de acciones y bloqueos automáticos en tiempo real
- Protección de plataformas o sistemas operativos que no cuentan con los parches de seguridad adecuados
- Optimiza y genera un mejor rendimiento dentro de trafico de red

4.1.7. Taxonomía reglas en un IDS.

Las reglas son un punto principal que ocupa a un IDS, de manera predeterminada viene algunas configuradas que pueden ser utilizadas. Sin embargo, es necesario conocer como es la elaboración de una nueva regla personalizada.

Tiene tres componentes principales acción, encabezado y opciones de la regla.

Figura 2. Componentes de una regla en un IDS.

Acción: si hay coincidencia se determina la acción a tomar.
Encabezado: se define el protocolo, direcciones de red, puertos y flujo de la red que será analizada.
Opciones: define las opciones y detalles de la regla.

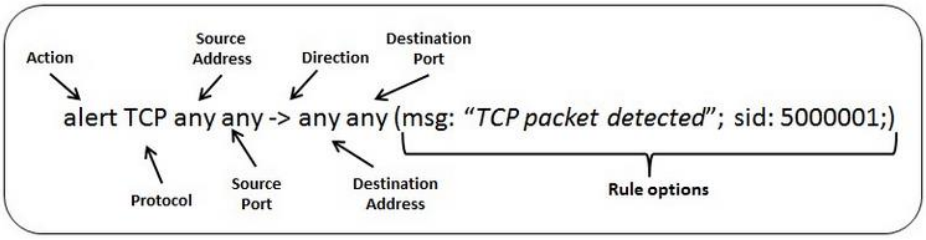


Figura 3. Taxonomía regla IDS.
Fuente: https://www.clavei.es/wp-content/uploads/Detectar-TCP.jpg

```
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;)
```

Figura 4. Ejemplo regla IDS.

En este ejemplo, el **rojo** es la acción, el **verde** es el encabezado y el **azul** son las opciones

Acciones
Alert - generar una alerta
Pass - detener la inspección adicional del paquete
Drop - soltar paquete y generar alerta
Reject: envía un error de falta de alcance RST/ICMP al remitente del paquete coincidente.
Rejectsrc- lo mismo que simplemente rechazar
Rejectdst: envía un paquete de error RST/ICMP al receptor del paquete coincidente.
Rejectboth: envía paquetes de error RST/ICMP a ambos lados de la conversación.

Encabezado
tcp (for tcp-traffic)
udp
icmp
ip (ip stands for 'all' or 'any')

Opciones
Msg: mensaje de alerta que emitira.
flow: flujo de red.

Content: contiene la cadena de caracteres que se debe buscar dentro del tráfico.
Reference: contiene referencias, parámetros y palabras clave.
Sid: ID de la regla identificada.
Rev: versión de la regla.
Classtype: brinda información sobre la clasificación de las reglas y alertas.

4.2 MARCO CONCEPTUAL

- Seguridad de la información: son aquellas medidas y contramedidas que se toman en conjunto con los procedimientos para proteger la integridad, confidencialidad y disponibilidad de la información.

- Seguridad informática: dentro de las ramas de la seguridad de la información encontramos como la seguridad informática procura proteger la infraestructura tecnológica y de comunicaciones.

- Seguridad lógica: para proteger de manera lógica todo aquel sistema informático como datos, aplicaciones, software, plataformas y sistemas operativos.

- Amenaza: son aquellos eventos que se generan de manera intencional ocasionando daño a sistema provocando perdida de algún tipo a la organización.

- Vulnerabilidad: es aquella debilidad que se pueden encontrar dentro de algún sistema informático, infraestructura de red, sistema operativo o base de datos que pude generar que un ciberdelincuente generé intrusiones a la organización.

- Ataque: es la acción que se genera al hacer uso de una vulnerabilidad y que puede permitir el control de un atacante al sistema.

- Ciber-atacante: individuo u organización que genera intrusiones a sistemas de información no autorizadas vulnerando la seguridad y genera daños dentro de las organizaciones.

- Falso positivo: es aquel tráfico inofensivo dentro de la red que no genera ningún impacto dentro de la organización y presenta una alarma falsa.

5 EVALUACIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS IDS DE CÓDIGO ABIERTO

Objetivo 1: Evaluar los sistemas de detección de intrusos IDS de código abierto existentes en el mercado permitiendo identificar las mejores opciones a trabajar dentro del proyecto de investigación.

Dentro de la valoración y evaluación de los IDS de código abierto para este caso se proponen dos de las soluciones más reconocidas Suricata y Snort.

5.1 SURICATA

Es un sistema basado en reglas y firmas que permiten el análisis de los paquetes de red en búsqueda de patrones, estas reglas deben estar actualizadas para lograr un constante monitoreo y fue desarrollado por la comunidad OISF (Open Information Security Foundation). Teniendo en su núcleo la posibilidad de realizar la detección de amenazas, de código libre, operando de una manera más rápida que otros IDS.

Otro de los aspectos más relevantes de Suricata es la capacidad de detección de intrusos en tiempo real, así como la posibilidad de realizar el monitoreo de red y la capacidad de procesamiento de los paquetes en red de una manera más eficiente haciendo uso de la capacitad de trabajo multi-hilo balacenado su carga de trabajo en todos los procesadores del sistema.

Haciendo uso de las configuraciones en sus reglas, el lenguaje de sus firmas bajo los comandos Lua (termino en portugués que significa Luna y es un lenguaje de secuencia de comandos) realiza una detección avanzada de malware permitiendo decodificar ese tráfico para su análisis.

Permite realizar integraciones con otras plataformas entre las que se encuentran los SIEM mediante los formatos YAML, JSON. Estos formatos también aplican como insumo de entrada a Suricata.

La comunidad existente de Suricata busca mantener la seguridad, usabilidad y eficiencia del código abierto.

A continuación, se mencionan varias características:

- Uso de varios núcleos en CPU, ejecutando varios subprocesos en simultanea
- Aceleración mediante el hardware, permitiendo operar con tarjetas GPU
- Análisis de archivos en tiempo real

- Generador de un motor de secuencias lo que permite generar varias reglas en un solo script LuaJIT
- Registro de certificados SSL, peticiones HTTP, solicitudes DNS
- Cuenta con una amplia comunidad
- Detección de protocolos automático
- IP Reputation, GeoIP
- JSON event and alert outputs
- Motores multipropósito NDIS, NIPS, NSM
- Compatibilidad con protocolos como TCP/IP, IPv4, Ipv6

Puede ser instalado bajo el sistema operativo GNU/Linux o Windows

5.2 SNORT

Este IDS es una de las principales soluciones de código abierto adoptada por varios fabricantes en el mundo por su capacidad de análisis de paquetes y detección de intrusos que se basa en red. Este análisis se realiza en tiempo real con una gran cantidad de reglas que son bastante potentes para este tipo de soluciones.

Contiene una gran variedad de patrones, reglas dentro de su configuración predeterminadas lo que permite tener un control más rápido dentro de la red, así como sus actualizaciones de manera continua por la comunidad.

Dentro de sus características encontramos las siguientes:

- Analiza varias fuentes.
- Realiza comparación del tráfico con los patrones de ataque.
- Puede realizar análisis estadísticos
- Motor de detección basado en reglas.
- Detección de anomalías dentro de la red
- Su capacidad de creación de reglas de manera sencilla
- Genera alertas y logs
- Existe un gran número de reglas pre-configuradas
- Integración con las salidas exportadas a BD, XML, TCPDUMP, syslog, winpopup, Socket
- Algunas ocasiones puede ser configurado como Honeypot
- Detecciones tipo SQL, Active X, cabeceras HTTP, Java/JavaScript, virus mediante las configuraciones de reglas.

5.3 COMPARATIVO CARACTERISTICAS

Existe diversas características entre estos dos IDS como por ejemplo la capacidad de crear sus propias firmas basados en los patrones de ataques dentro de la red y es posible utilizar diferentes módulos mediante los plugins, la capacidad de detección de malware entre otras, la siguiente tabla ilustra ambas soluciones.

Características	**Snort**	**Suricata**
Desarrollador	Cisco	Open Information Security Foundation
Licencia	GPLv2	GPLv2
Soporte Multiplataforma	Sí	Sí
Sistema operativo	Linux, Unix, Windows, MacOS	Linux, Unix, Windows, MacOS
Modos de funcionamiento	Inline y en línea pasiva	Inline y en línea pasiva
Motor de detección	Basado en reglas	Basado en reglas
Soporte de reglas	Compatible con reglas de Snort	Compatible con reglas de Snort
Número de reglas	Más de 11,000	Más de 40,000
Escalabilidad	Escalabilidad vertical limitada	Escalabilidad horizontal y vertical
Funcionalidades	Detección de intrusiones, prevención de intrusiones, registro de eventos, captura de paquetes, análisis de tráfico, entre otros.	Detección de intrusiones, prevención de intrusiones, registro de eventos, captura de paquetes, análisis de tráfico, análisis de malware, entre otros.
Lenguajes de reglas	Snort y Emerging Threats open	Suricata y Emerging Threats open
Rendimiento	Bajo rendimiento en comparación con Suricata	Alto rendimiento
Soporte de protocolos	TCP, UDP, ICMP, HTTP, DNS, FTP, SMTP, SSH, SIP, SSL, entre otros.	TCP, UDP, ICMP, HTTP, FTP, TLS (THIS INCLUDES SSL), SMB, DNS, DCERPC, SSH, SMTP, IMAP, MODBUS (DISABLED BY DEFAULT), DNP3 (DISABLED BY DEFAULT), ENIP (DISABLED BY DEFAULT), NFS, IKEV2, KRB5, NTP, DHCP, RFB, RDP, SNMP, TFTP, SIP, HTTP2.
Velocidad de procesamiento	5-10 Gbps	10-20 Gbps
Fácil configuración	Fácil de configurar	Más complejo que Snort
Gestión de eventos	Soporte limitado	Soporte completo
Soporte de salida	Soporte limitado	Soporte completo
Flexibilidad	Limitada	Mayor

Comunidad	Grande y activa	Grande y activa

Tabla 1: Evaluación sistemas de detección de intrusos - IDS

Según la tabla anterior y la valoración dentro de las características de los IDS evaluados, se evidencia un que el más idóneo que cumple con el mayor rendimiento, capacidades, cantidad de reglas, velocidad de procesamiento y mejor escalabilidad es Suricata.

Dentro de la comunidad es posible recibir las nuevas actualizaciones de otras firmas creadas por otros usuarios. Este IDS está disponible para realizar su instalación en ambientes Windows y GNU/Linux.

6 PRUEBAS IDS IDENTIFICANDO EL GRADO DE DIFICULTAD DURANTE SU IMPLEMENTACIÓN

Objetivo 2: Desarrollar pruebas con los IDS mejor evaluados permitiendo identificar las curvas de aprendizaje y grado de dificultad en su implementación.

Para lograr desarrollar este objetivo y permitiendo identificar su facilidad al momento de la implementación se describen los requisitos necesarios para cada uno de los IDS.

6.1 REQUISITOS PARA LA IMPLEMENTACIÓN DE UN IDS – SURICATA

Se tiene en cuenta dos soluciones de código abierto para la implementación de un IDS, la primera de ellas es SURICATA que requiere los siguientes requisitos como se muestra en la figura 2, donde se muestra la capacidad para realizar la instalación en diversos sistemas operativos.

Figura 5. Suricata versión y características
Fuente: https://suricata.io/features/

Dentro de los sistemas operativos compatibles para realizar la instalación se encuentran los siguientes:

- Microsoft Windows
- RHEL/CentOS 8 and 7
- Fedora
- Debian
- Ubuntu

6.2 REQUISITOS PARA LA IMPLEMENTACIÓN DE UN IDS – SNORT

SNORT requiere los siguientes requisitos a nivel de maquina y sistemas operativos soportados para su implementación.

Sistemas operativos:

Alpine 3.14/x86-64
Alpine 3.15/x86-64
CentOS 7/i386
CentOS 7/x86-64
CentOS 8/x86-64
Debian 10/i386
Debian 10/x86-64
Debian 11/x86-64
Fedora Core 35/x86-64
FreeBSD 13/x86-64

OpenBSD 6.9/x86-64
OpenBSD 7.0/x86-64
OpenSUSE LEAP 15.3/x86-64
RHEL 7/x86-64
RHEL 8/x86-64
Slaceware 14.2/x86-64
Ubuntu 14/i386
Ubuntu 14/x86-64
Ubuntu 16/i386
Ubuntu 16/x86-64
Ubuntu 18/x86-64
Ubuntu 20.04/x86-64
Ubuntu 21.14/x86-64

Entornos virtuales donde es posible instalar el IDS:

- VirtualBox
- Xen
- Vmware

Para la asignación de memoria se debe tener en cuenta cual es la cantidad del tráfico de red que se desea monitorear ya que estos procesos pueden consumir bastante memoria RAM y CPU.

Durante el proceso de evaluación de los IDS mencionados en la investigación se obtiene los siguientes resultados.

características	**Snort**	**Suricata**
Multi hilo (Threading)	No	Si
Soporte Ipv6	Si	Si
Reputación IP	No	Si
Detección automática protocolos	No	Si
Aceleración GPU	No	Si
GeoIP	No	Si
Variables Globales/Flowbits	No	Si
Análisis avanzado de HTTP	No	Si
HTTP acces logging	No	Si
SMB Acces logging	No	Si
Detección de alertas basado en reglas	Si	Si
Gratuito	Si	Si

Tabla 2: Comparativo de características IDS

Es importante para iniciar las pruebas conocer los escenarios y topologías base que regularmente se encontrara en una Pyme, el siguiente diagrama permite identificar los equipos que se involucran dentro de una red y la ubicación del IDS.

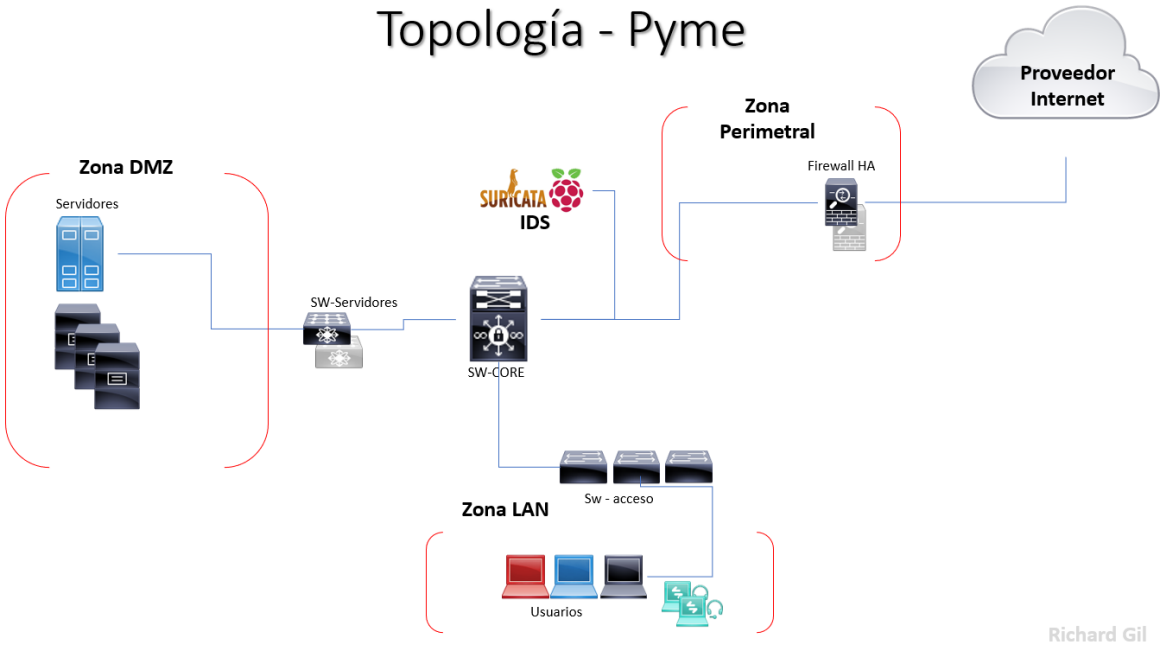


Figura 6: Topología de red en una Pyme.
Fuente: Elaboración propia

El siguiente flujo muestra cómo funciona el motor de detección de un IDS

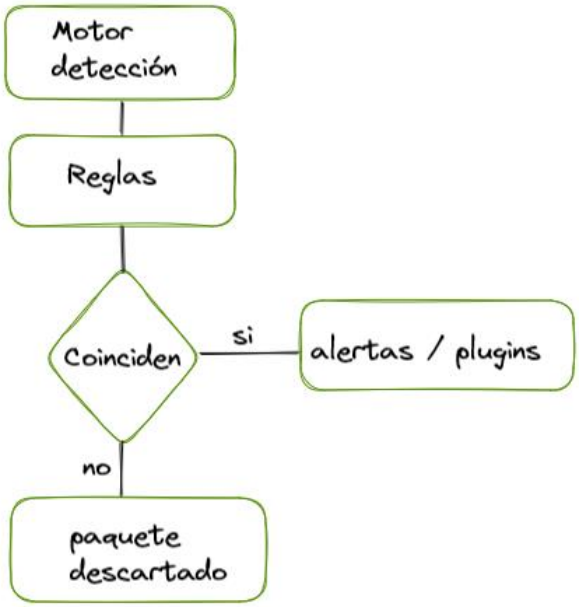


Figura 7. Flujo motor de detección
Fuente: Elaboración propia

6.3 SINGLE BOARD

Debemos mencionar que los single board son computadoras completas que se encuentran en una sola placa de circuito impreso. Están diseñados para funcionar como una computadora completa, con todos los componentes esenciales, como procesador, memoria, almacenamiento y conectividad integrados en una sola placa.

La función principal de los single board es proporcionar una solución de bajo costo y alta eficiencia para aplicaciones informáticas específicas. Se utilizan comúnmente en proyectos de electrónica, robótica, automatización del hogar, sistemas de control industrial, educación y muchos otros campos. También son populares entre los entusiastas de la tecnología que disfrutan construyendo sus propias computadoras personalizadas.

En esta topología es importante ubicar entre la zona perimetral y el CORE principal la Raspberry con el servicio de IDS, permitiendo identificar todos los paquetes que viajan dentro de la RED.

Adicional es posible ubicar otro Raspberry de manera opcional del lado de la zona de servidores o la zona LAN si se desea un control mucho más granular y detallado de todo el tráfico de las redes.

En este caso usaremos un dispositivo de bajo costo (Single Board) denominado Raspberry Pi B, que tiene las siguientes características como lo muestra la imagen.

Figura 8. Raspberry pi
Fuente: https://images.prismic.io/rpf-products/877fb653-7b43-4931-9cee-977a22571f65_3b%20Angle%202%20refresh.jpg?ixlib=gatsbyFP&auto=compress%2Cformat&fit=max&w=600&h=400

- Broadcom BCM2837 64bit Quad Core Processor powered Single Board Computer running at
- 1.2GHz 1GB RAM
- BCM43438 WiFi on board
- Bluetooth Low Energy (BLE) on board
- 40pin extended GPIO
- 4 x USB 2 ports
- 4 pole Stereo output and Composite video port
- Full size HDMI CSI camera port for connecting the Raspberry Pi camera
- DSI display port for connecting the Raspberry Pi touch screen display

- Micro SD port for loading your operating system and storing data
- Upgraded switched Micro USB power source (now supports up to 2.4 Amps)
- Same form factor as the Pi 2 Model B, however the LEDs have changed position

6.4 EVALUACION IDS

Para generar la valoración correspondiente se consideran las variables de funciones, desempeño y seguridad.

6.4.1 Variable Funciones

Para proceder con la valoración de la variable se genera la siguiente tabla con valores entre 0 y 5 cubriendo los criterios mas relevantes referente a las funciones de los IDS.

Criterio	Snort	Suricata
Escalabilidad	4	5
Protocolos de red	4	5
Multi Hilo	2	4
Soporte IpV6	5	5
Complementos	5	5
Detección por reglas	5	5
Reputación de IP	5	5
Modulo GeoIP	0	5
Promedio	**3,75**	**4,87**

Tabla 3: Valoración indicador de funciones

Se observa la valoración en promedio teniendo a SNORT con un promedio de 3,75 y Suricata con 4,87, estas fueron realizadas operando sobre los dispositivos de bajo costo.

A nivel porcentual se observa que Snort tiene un 75% y Suricata con un 97,5% a nivel funcional, siendo Suricata mejor valorado frente a las funciones.

6.4.2 Variable desempeño

Se realiza una valoración durante los tiempos de entrenamiento de los IDS, incluyendo paquetes que contienen amenazas obteniendo los siguientes resultados. En este apartado es importante resaltar una de las funciones principales de Suricata y es su capacidad de procesamiento multi-hilo lo que hace que sea más eficiente y rápido durante los análisis a los paquetes de red.

En el análisis realizado mediante Snort se encuentran algunas perdidas en los paquetes de red y los tiempos de respuesta son mas elevados, por el lado de Suricata no hay perdida de paquetes y los tiempos son mucho más cortos.

La siguiente tabla muestra el resultado obtenido durante el proceso.

Criterio	Snort	Suricata
Tiempo de respuesta	3	5
Paquetes perdidos	3	5

Tabla 4: Valoración indicador de desempeño

Suricata muestra un mejor desempeño frente a los tiempos de respuesta sin pérdida de paquetes durante la valoración.

6.4.3 Variable Seguridad

Se procede a realizar la valoración de los criterios mas relevantes frente a la seguridad que se tiene con los IDS.

Criterio	Snort	Suricata
Extracción de archivos	0	5
Lua – Motor scripting	4	5
Peticiones DNS	2	4
Peticiones HTTP	5	5
Capturar certificados TLS/SSL	5	5
Decodificación de paquetes	5	5
Promedio	**3,5**	**4,8**

Tabla 5: Valoración indicador seguridad

Se puede evidenciar que el promedio por parte de Snot es de 3,5 lo que representa un 84% y para el caso de Suricata es un promedio de 4,8 que corresponde a un 97%.

7 PROCEDIMIENTO DE IMPLEMENTACIÓN DE UN IDS DE CÓDIGO ABIERTO - GUIA PARA LAS PYMES

A continuación, se listan los equipos que son requeridos para la instalación.

- Raspberry Pi 3
- MicroSD 16gb
- Cables de red
- Conexión a internet
- Pc o portátil

Iniciamos con el proceso de descarga del instalador para Windows Raspberry Pi Imager desde el siguiente link [4].

Para cargar el sistema operativo Debian 10 en la Micro SD ejecutamos el Raspberry Pi Imager como muestra la siguiente figura.

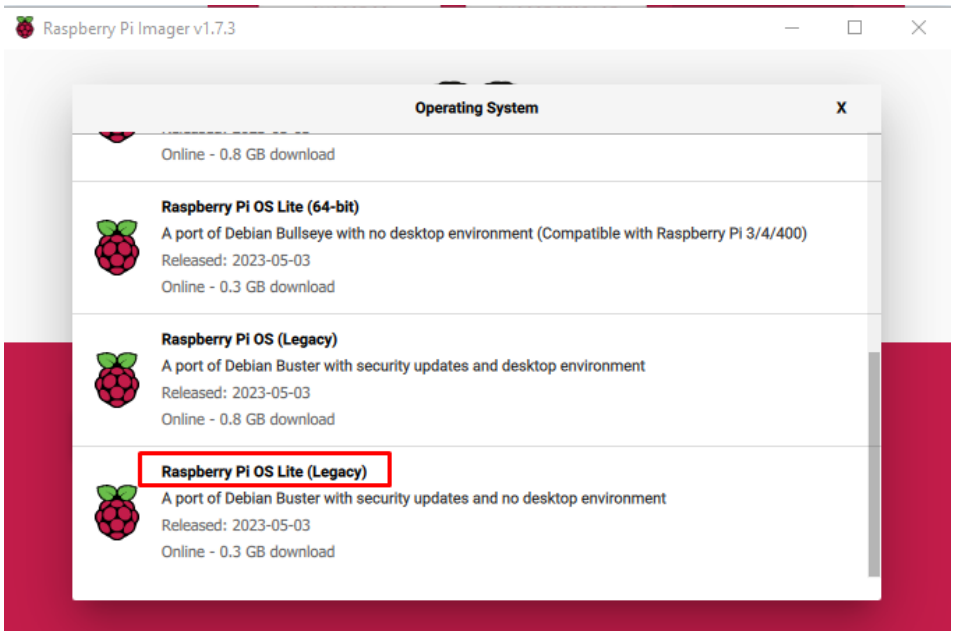


Figura 9: Cargando el SO Debian en MicroSD

También es posible realizar la descarga del sistema Linux para la instalación de manera manual desde el siguiente link[5], Debian búster 10.12.

[4] https://www.raspberrypi.com/software/
[5] https://www.raspberrypi.com/software/operating-systems/#raspberry-pi-os-legacy

En este punto ya es posible inicializar la Raspberry Pi y tendremos el sistema operativo corriendo totalmente operativo.

Con el sistema instalado se procede a realizar la instalación de suricata con los siguientes comandos que pueden ser tomados como instructivo para una configuración.

Instalación dependencias requeridas

Se deben ejecutar los siguientes comandos sobre la consola Shell en Raspberry.

sudo apt install libpcre3 libpcre3-dbg libpcre3-dev build-essential libpcap-dev libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev make libmagic-dev libjansson-dev rustc cargo python-yaml python3-yaml liblua5.1-dev

Descargar empaquetado de suricata

wget https://www.openinfosecfoundation.org/download/suricata-6.0.6.tar.gz

Desempaquetar el paquete y abrir la carpeta correspondiente

ejecutar el siguiente comando para configurar los parámetros de instalación dentro de la carpeta de descarga del paquete

./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var --enable-nfqueue --enable-lua

Realizar la compilación

Ejecutar el siguiente comando dentro de la carpeta

make

Iniciar el proceso de instalación

sudo make install

cambiar de directorio a la carpeta de actualización

cd $HOME/suricata-6.0.6/suricata-update/

Compilar suricata-update

sudo python setup.py build

instalar suricata update

sudo python setup.py install

para finalizar nuevamente cambiamos de directorio

cd $HOME/suricata-6.0.6/

Incluir las reglas de suricata

sudo make install-full

Actualizar reglas

sudo suricata-update

Para ejecutar las configuraciones necesarios es necesario realizar algunos cambios en el archivo.yaml

sudo vi /etc/suricata/suricata.yaml

la variable HOME_NET contiene las redes o segmentos que se desean monitorear

HOME_NET: "[192.168.0.0/24]"

Inicializando la ejecución de suricata

- -c <ruta>: archivo de configuración a usar
- -i <interfaz>: interfaz Ethernet para monitorear
- -S <ruta>: archivo que contiene las reglas a utilizar

sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -S /var/lib/suricata/rules/suricata.rules

En este punto ya se está ejecutando y realizando los análisis dentro de la red, para visualizar los registros que se están generando.

Desde la salida del log se evidencia los registros a nivel de red y los alertas que este haciendo match con alguna de las reglas mediante el comando.

sudo tail -f /var/log/suricata/fast.log

Con el IDS ya operando en el equipo de pude realizar diversas pruebas que permiten validar las reglas y alertas que recién están configuradas.

Por ejemplo, una regla personalizada que detecte cuando se esta realizando ping hacia el mismo IDS, esto automáticamente genera una alerta sobre el equipo como se puede evidenciar en la imagen.

```
alert icmp any any -> any any (msg: "ICMP detected...";)
```

Figura 10: Regla personalizada monitoreo ICMP

En la parte izquierda se envía la petición de ping mediante el ICMP, en la parte derecha como el IDS lo detecta según la regla personalizada que se configuro.

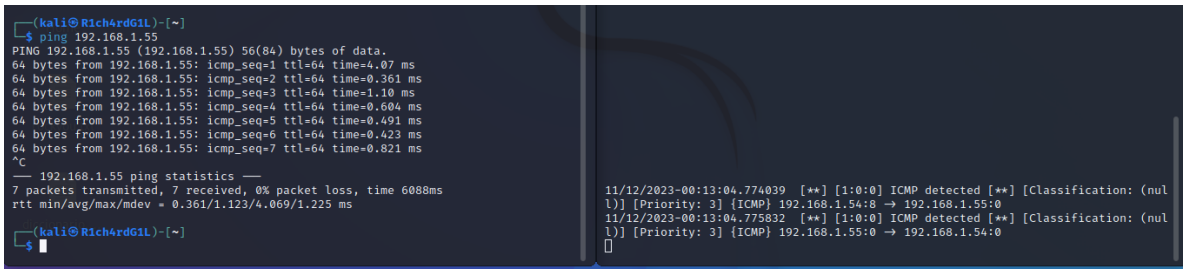


Figura 11: Alerta detectada por el IDS mediante PING

El IDS tiene sus propias reglas que constantemente se están actualizando lo que aporta a las PYMES estar a la vanguardia con las nuevas amenazas que se puedan presentar.

Durante los procesos de intrusión los ciber-delincuentes buscan realizan análisis de puertos para posterior a ello intentar realizar movimientos laterales o explotación de vulnerabilidades, es en este punto donde el IDS esta monitoreando estos comportamientos constantemente. La siguiente imagen muestra en la izquierda un escaneo de vulnerabilidades y como el IDS lo detecta en la parte derecha.

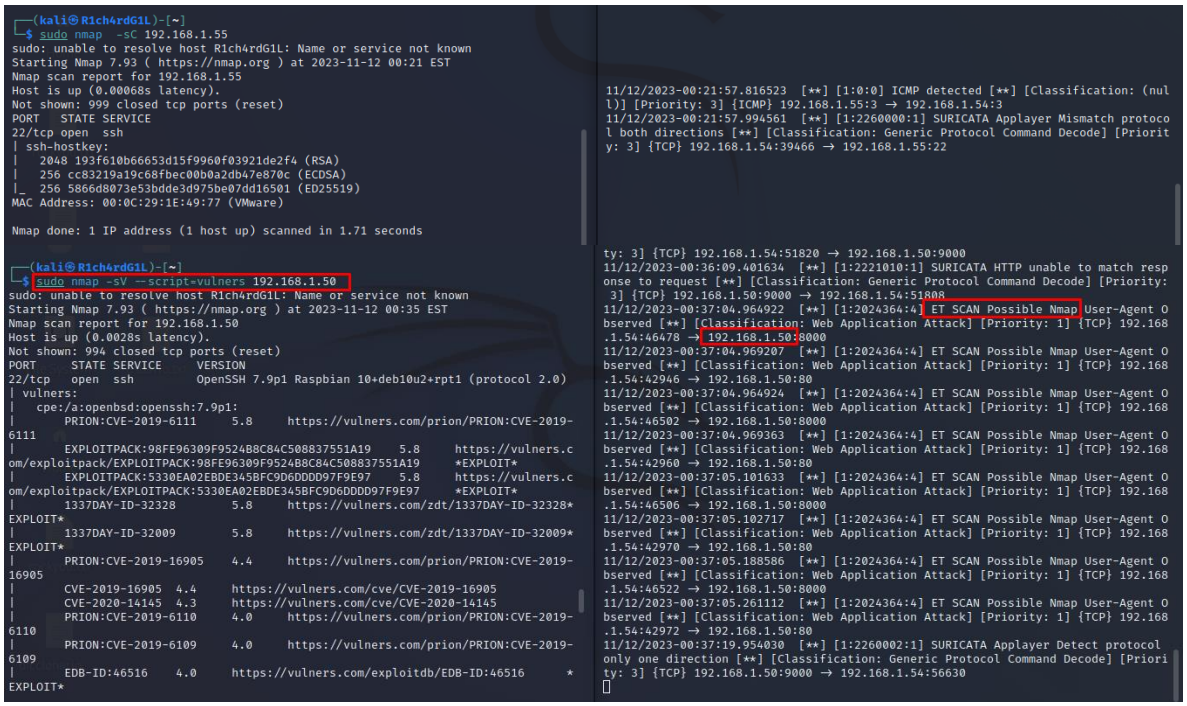


Figura 12: Alerta detectada por el IDS por escaneo de vulnerabilidades

Dentro de las reglas se pueden identificar cuando algún equipo trata de acceder a la DEEP WEB mediante la red TOR al buscar los DNS .onion.

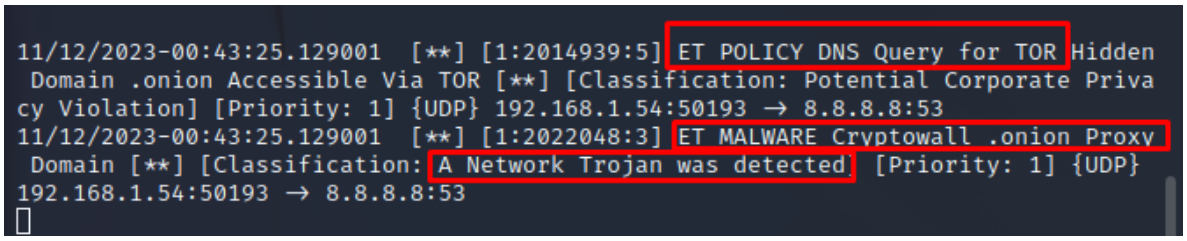


Figura 13: Alerta detectada por el IDS al acceder los DNS .onion

Adicional tenemos un constante monitoreo sobre las reglas cuando se trata de descargar archivos con código malicioso o virus como muestra la alerta del IDS, en la parte izquierda se intenta navegar hacia una url que contiene un archivo con virus y en la parte derecha como el IDS genero la alerta correspondiente.

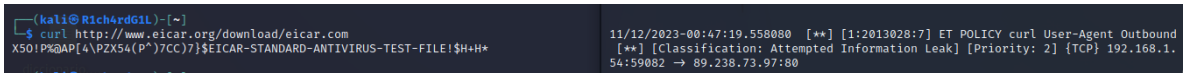


Figura 14: Alerta detectada por el IDS al intentar descargar un archivo con virus

8 RECOMENDACIONES

La implementación de soluciones de software libre como IDS (Sistemas de Detección de Intrusión) en dispositivos de bajo costo puede ser una opción eficaz para las pymes que desean mejorar su seguridad cibernética sin incurrir en grandes gastos.

A continuación, unas pautas que sirven de ayuda en este escenario y podría ser un paso a paso sobre cómo las pymes pueden llevar a cabo el proceso de adopción de este tipo de soluciones.

- **Evalúa tus necesidades de seguridad:** Antes de comenzar, la Pyme identifica sus necesidades de seguridad cibernética específicas. ¿Qué activos necesitas proteger? ¿Cuáles son tus principales preocupaciones de seguridad?

- **Investiga soluciones de software libre de IDS:** Investiga y selecciona una solución de software libre de IDS que se ajuste a tus necesidades. Ejemplos populares incluyen Snort, Suricata, y Bro/Zeek entre otras, sin dejar de lado las que tienen otro tipo de licenciamiento.

- **Selecciona hardware de bajo costo:** Busca hardware de bajo costo para ejecutar el IDS. Puedes utilizar Single Board de diferentes fabricantes si cumple con los requisitos mínimos de sistema de la solución IDS.

- **Instala el sistema operativo:** Instala un sistema operativo adecuado para el hardware seleccionado. Las distribuciones de Linux como Ubuntu Server o CentOS son opciones comunes y compatibles.

- **Descarga e instala el IDS:** Descarga e instala la solución IDS según el sistema operativo. Seguir las instrucciones proporcionadas por la comunidad o el sitio web oficial del proyecto de software libre.

- **Configura el IDS:** Configura las reglas y políticas de detección de intrusiones según tus necesidades específicas. Asegurarse de optimizar el IDS para minimizar falsos positivos.

- **Implementa el IDS en tu red:** Conecta el hardware con el IDS configurado en tu red. Asegúrate de que esté en una ubicación estratégica para monitorear el tráfico de red entrante y saliente. Esto dependerá mucho de la zona que se desee monitorear dentro de la red o segmentos de red.

- **Realiza pruebas y ajustes:** Llevar a cabo pruebas exhaustivas para verificar que el IDS esté funcionando correctamente. Ajustar las configuraciones según sea necesario para no generar falsos positivos.

- **Configura alertas y notificaciones:** Configura alertas y notificaciones para que el personal de seguridad o administradores sean informados inmediatamente cuando se detecten posibles intrusiones o alteraciones en la red.

- **Mantenimiento y actualizaciones:** Realizar un mantenimiento regular del IDS, incluyendo actualizaciones de software y reglas de detección. Mantén el sistema operativo y el hardware en buen estado.

- **Capacitación del personal:** Proporcionar capacitación al personal para que comprendan cómo funciona el IDS y cómo responder ante incidentes de seguridad. Importante este proceso de sensibilización al interior.

- **Monitorización continua:** Establecer un proceso de monitoreo continuo para supervisar las alertas y los registros generados por el IDS y tomar medidas en consecuencia.

- **Evaluación periódica:** Evaluar regularmente la efectividad del IDS y ajustar las configuraciones según sea necesario para mantener la seguridad de la red.

- **Documentación y registro:** Llevar un registro de todas las configuraciones, cambios y eventos relacionados con el IDS para futuras auditorías y referencia.

- **Comunidad y soporte:** Unirse a la comunidad de usuarios de la solución IDS que estés utilizando y aprovecha los recursos de soporte y las actualizaciones de seguridad.

La implementación de un IDS basado en software libre en dispositivos de bajo costo puede ser una forma efectiva y económica de mejorar la seguridad cibernética en las pymes. Sin embargo, es importante recordar que la seguridad es un proceso continuo y que se deben tomar medidas adicionales, como la gestión de parches y actualizaciones, para mantener un nivel óptimo de seguridad a lo largo del tiempo.

Basado en el estudio previo realizado se logra determinar que la implementación de un IDS permite tener el entorno de lo que ocurre a nivel de red, mediante las configuraciones y afinamientos de cada escenario para cada organización de manera que se genere una capa adicional se seguridad frente a los ataques informáticos.

El IDS se puede colocar de las siguientes formas:

- Frente al Firewall
- Detrás del Firewall
- Combinación de ambos
- Modo NIPS

En otros escenarios se puede colocar mediante puertos espejos del switch o routers y se coloca de manera paralela a la red.

Es importante contar con una solución IDS que permita evidenciar dentro de la red cual es el comportamiento de los paquetes que viajan dentro de la misma,

9 CONCLUSIONES

La implementación de un IDS con dispositivos de bajo costo puede ser una estrategia efectiva para mejorar la seguridad cibernética en las Pymes, especialmente cuando los recursos financieros son limitados. Sin embargo, es importante recordar que la seguridad cibernética es un esfuerzo continuo y que la combinación de tecnología, procesos y concienciación del personal es esencial para proteger la empresa de manera efectiva.

El código abierto abre una gran posibilidad para la implementación de soluciones como IDS para cualquier tipo de empresa independiente su sector y actividad económica. Es importante que dentro de las características del código abierto se cuente con el apoyo de la comunidad para mantener el proyecto en las mejores condiciones y lo más actualizado posible.

La variedad de IDS es bastante amplia cada uno con sus ventajas y desventajas sin embargo para las Pymes es una gran herramienta el poder contar con soluciones de este tipo que permitan tener una visión más detallada de lo que ocurre al interior dentro de las redes.

Las organizaciones hoy en día están centralizando sus procesos, así como las infraestructuras, es en este punto donde es necesario tener una solución como un IDS que permita tener un monitoreo y supervisión del tráfico de red que se genera al interior de la red local.

La implementación de un IDS se cuenta como una herramienta que luego de realiza su instalación y afinamiento con conocimiento de redes y la programación realizada en sus políticas y reglas, permitirá tener una visualización en tiempo real del tráfico de red.

El flujo de trafico de una red es bastante grande por lo que se deben hacer algunos ajustes en la configuración para no tener perdida de paquetes, adicional el ser un proceso multihilo dependerá de la cantidad de tráfico que el dispositivo tenga que analizar para obtener una respuestas más rápida y fluida.

Es posible integrar varios plugins adicionales que permitan tener una mejor compresión de los eventos que ocurren dentro de la red.

Se puede realizar modificaciones en la cantidad del tamaño utilizado para los logs lo que permite tener un histórico mucho más amplio dentro del dispositivo.

Durante las pruebas se logra validar que los dos IDS usan dentro de sus funciones principales los análisis del trafico basado en firmas de conocimiento.

La valoración de los indicadores de funciones muestra que Snort tiene un 75% mientras que Suricata un 97,5%, lo que indica que esta por encima de 22,5%. Teniendo una mayor cobertura en funcionabilidades.

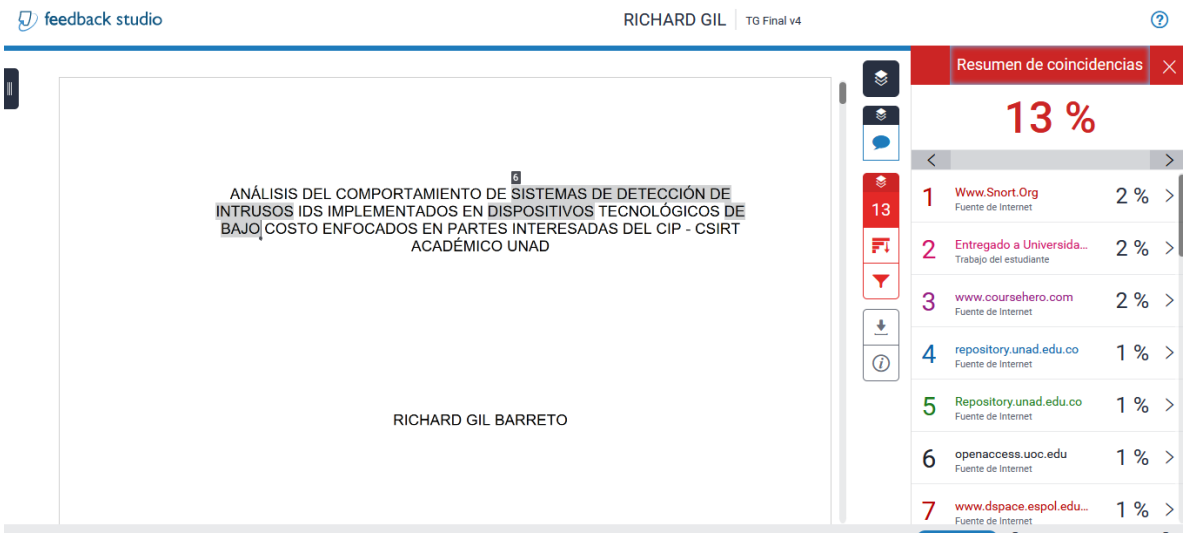
Para la valoración realizada sobre el rendimiento se evidencia que Suricata tiene un mejor desempeño precisamente por algunas diferencias en sus características como el manejo de multi-hilos al momento de realizar el procesamiento interno del tráfico.

La seguridad es un factor importante al momento de hacer uso de IDS ya que permite Snort y Suricata realizar un análisis de paquetes mediante la decodificación y análisis del tráfico, así como el análisis de algunos archivos que pueden ser catalogados como maliciosos.

10 ANEXOS

Link video
https://tinyurl.com/2p8b6yp2

Prueba anti plagio



11 BIBLIOGRAFÍA

BIRKINSHAW, Celyn. ROUKA, Elpida y VASSILAKIS, Vassilios G. Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. En: Journal of Network and Computer Applications [en línea]. Junio, 2019. vol. 136 [consultado el 17 abril, 2022]. p. 71-85. Disponible en: https://doi.org/10.1016/j.jnca.2019.03.005

CSIRT, Incibe. Diseño configuración ips ids siem en sci. [en línea]. Noviembre 2017. [consultado el 15 de abril de 2022], Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/certsi_diseno_configuracion_ips_ids_siem_en_sci.pdf

CSIRT, Incibe. ¿Qué son y para qué sirven los SIEM, IDS e IPS?. [en línea]. Septiembre 2020. [consultado el 17 de abril de 2022], Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

FRIAS MENA, Daniel. ELÍAS ÁLVAREZ, Yaima de los Ángeles. MACHADO GARCÍA, Yendry. Módulo de gestión de reglas de detección para el IDS Snort. Enero 2015. [en línea]. [Consultado el 20 de abril 2023]. Disponible en: https://repositorio.uci.cu/jspui/handle/ident/8338

GÓMEZ FERNÁNDEZ, Sadoht. Implementación de un IDS de bajo coste para uso doméstico o en la pequeña empresa. [en línea]. Diciembre 2019. [consultado el 17 de abril de 2022]. Disponible en: http://hdl.handle.net/10609/107246

LIMA, Felipe dos Anjos. Implantação e análise de desempenho de um cluster com processadores ARM e plataforma raspberry Pi [en línea]. 2016 [consultado el 14 de abril de 2022]. Disponible en: https://ri.ufs.br/handle/riufs/3378.

MARTINEZ SOLARTE, Guillermo, OCAMPO, Carlos, CASTRO BERMÚDEZ, Yanci. Sistema de detección de intrusos en redes corporativas. Sci Tech. [en línea]. Marzo 2017 [Consultado el 17 de abril de 2022] Disponible en: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/9105

MEDINA MORENO, Juan Carlos. Prospectiva de las políticas gubernamentales del modelo de financiación en el crecimiento de las Pymes en Colombia. En: Contexto [en línea]. diciembre 2019. vol. 8 [consultado el 17 febrero 2022]. Disponible en: https://doi.org/10.18634/ctxj.8v.0i.980

MOSCOTE MEDINA, Rafael. Sistema de detección y prevención de intrusos IPS para la Vlan de servidores de la Sociedad Minera de Santander S.A.S. en Bucaramanga (Santander). [en línea]. 2017. [consultado el 22 de abril de 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/14341

PANTOJA DARIO, Nelson, AMADOR DONADO, Siler, MARCELES VILLALBA, Katerine. Selección de indicadores para la implementación de un IDS en PYMES. [en línea]. 2019. [Consultado el 18 de abril de 2023]. Disponible en: https://www.proquest.com/openview/ddddee94d23b4c4a6d43646933893d01/1?pq-origsite=gscholar&cbl=1006393

SOLARTE MARTINEZ, Guillermo Roberto; OCAMPO, Carlos Alberto y CASTRO BERMÚDEZ, Yanci Viviana. Sistema de detección de intrusos en redes corporativas. [en línea]. Marzo 2017. [consultado el 17 de abril de 2022]. Disponible en: https://doi.org/10.22517/23447214.9105

SOUCASE IRANZO, Adrián. Implementación de un Sistema de Prevención de Intrusiones (IPS) en un modelo de red industrial. [en línea]. 2021. [Consultado el 11 de abril de 2022]. Disponible en: https://riunet.upv.es/handle/10251/178959

UPTON EBEN, Gareth. The “unofficial official” guide to the Raspberry Pi, complete with creator insight. [en línea]. Septiembre 2019. [consultado el 17 de abril 2022], 312p. Disponible en: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119415572.index

VILLALON HUERTA, Antonio. Seguridad en Unix y redes. [en linea]. Julio 2002. [Consultado el 12 de abril de 2022] Disponible en: https://www.rediris.es/cert/doc/unixsec/unixsec.pdf