UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

"DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS A TRAVÉS DE REDES DEFINIDAS POR SOFTWARE PARA IDENTIFICAR TRÁFICO MALICIOSO"

Trabajo de Investigación previo a la obtención del Título de Magíster en Telecomunicaciones

DIRECTOR:

Msc. Fabián Geovanny Cuzme Rodríguez.

ASESOR:

PhD. Iván Danilo García Santillán

AUTOR:

Ing. Marcelo Wladimir León Gudiño

IBARRA - ECUADOR

2021

APROBACIÓN DEL TUTOR

Yo, Fabián Geovanny Cuzme Rodríguez, certifico que el estudiante Marcelo Wladimir León Gudiño con cédula N° 1003636717 ha elaborado bajo mi tutoría la sustentación del trabajo de grado titulado "DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS A TRAVÉS DE REDES DEFINIDAS POR SOFTWARE PARA IDENTIFICAR TRÁFICO MALICIOSO"

Este trabajo se sujeta a las normas y metodologías dispuestas en el reglamento del título a obtener, por lo tanto, autorizo la presentación a la sustentación para la calificación respectiva.

Ibarra, 16 de diciembre de 2021

MSc. Fabián Geovanny Cuzme Rodríguez
Tutor
CI: 1311527012

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1.- IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO	
Cédula de Identidad	100363671-7
Apellidos y Nombres	León Gudiño Marcelo Wladimir
Dirección	Juan de Salinas y Eusebio Borrero Portal de Salinas
E-mail	mwleong@utn.edu.ec
Teléfono Fijo	062603310
Teléfono Móvil	0991329677
DATOS DE LA OBRA	
Título	DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS A TRAVÉS DE REDES DEFINIDAS POR SOFTWARE PARA IDENTIFICAR TRÁFICO MALICIOSO
Autor	León Gudiño Marcelo Wladimir
Fecha: DD/MM/AA	16/12/2021
Programa de posgrado	Maestría en Telecomunicaciones
Título por el que opta:	Magíster en Telecomunicaciones
Tutor	MSc. Fabián Geovanny Cuzme Rodríguez

2. CONSTANCIAS

El autor Marcelo Wladimir León Gudiño, manifiesta que la obra objeto de la presente autorización es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 16 días de diciembre de 2021

Marcelo Wladimir León Gudiño
CI: 1003636717

DEDICATORIA

Este proyecto lo dedico a mis padres Susana y Marcelo, a mis hermanas Susy, Belén y especialmente a mi hermana Gaby quién desde el cielo me guía en cada etapa de mi vida. Con cada granito de arena que aportó mi familia, con su esfuerzo, consejos, valores, su buen ejemplo y comprensión ha sido mi motivación para superarme cada día como persona y profesional y no dejarme vencer por ninguna adversidad, para ellos con todo mi amor y cariño.

Marcelo León

RECONOCIMIENTO

A mi director de trabajo de grado, Msc. Fabián Cuzme por su esfuerzo y dedicación, quien con su experiencia y conocimiento supo guiarme en la terminación de este proyecto.

A mi asesor de trabajo de grado, PhD, Iván García Santillán un cordial agradecimiento por brindar sus conocimientos que sirvieron para la culminación de este proyecto.

A la Universidad Técnica del Norte y al Instituto de Posgrado, por haberme brindado las herramientas y conocimientos necesarios para el cumplimiento de mis años de estudio y formación profesional de cuarto nivel.

Al Proveedor de Servicios de Internet SITEC SA por la confianza de sus dirigentes al permitir el desarrollo e implementación de mi trabajo de titulación en sus instalaciones.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DEL NORTE INSTITUTO DE POSGRADO PROGRAMA DE MAESTRÍA

"DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS A TRAVÉS DE REDES DEFINIDAS POR SOFTWARE PARA IDENTIFICAR TRÁFICO MALICIOSO"

Autor: Marcelo Wladimir León Gudiño

Tutor: Msc. Fabián Cuzme Rodríguez

Año: 2021

RESUMEN

El presente trabajo se realizó con el objetivo de desarrollar un Diseño de un sistema de detección de intrusos a través de redes definidas por software para identificar tráfico malicioso, la propuesta sirve para mejorar los sistemas de seguridad de los Proveedores de Servicios de Internet, la misma que es capaz de ser utilizada como guía para los profesionales de la rama correspondiente a las tecnologías de la información. El tráfico malicioso se identificó en base a la norma ISO 27005 mediante la interpretación de los riesgos acorde a los tipos de ataques cibernéticos, de donde se tomaron las directrices generales para la realización de cada uno de los niveles de seguridad. La validación del diseño se realizó mediante la aplicación de todas las actividades definidas por la metodología Offensive Security para el proceso de intrusiones en un escenario de simulación controlado. Se propone la implementación de la herramienta Mininet y el controlador RYU para la implementación de una red SDN. Adicional a la solución a la problemática planteada, se implementa un mecanismo de detección de ataques IDS en una red SDN, el cual detecta el tráfico malicioso.

Palabras clave: SEGURIDAD, SDN, IDS, ISO27005, RYU.

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO PROGRAMA DE MAESTRÍA

"DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS A TRAVÉS DE REDES DEFINIDAS POR SOFTWARE PARA IDENTIFICAR TRÁFICO MALICIOSO"

Autor: Marcelo Wladimir León Gudiño

Tutor: Msc. Fabián Cuzme Rodríguez

Año: 2021

ABSTRACT

The present work was carried out with the objective of developing a Design of an intrusion detection system through software-defined networks to identify malicious traffic, the proposal serves to improve the security systems of Internet Service Providers, the same which is capable of being used as a guide for professionals in the field of information technology. Malicious traffic was identified based on the ISO 27005 standard by interpreting the risks according to the types of cyber attacks, from which the general guidelines were taken to carry out each of the security levels. The design validation was carried out by applying all the activities defined by the Offensive Security methodology for the intrusion process in a controlled simulation scenario. The implementation of the Mininet tool and the RYU controller is proposed for the implementation of an SDN network. In addition to the solution to the problem raised, an IDS attack detection mechanism is implemented in an SDN network, which detects malicious traffic.

Keywords: SECURITY, SDN, IDS, ISO27005, RYU.

CAPITULO I

EL PROBLEMA

1.1.Problema de investigación

La seguridad de la información es un factor importante que se debe tener en consideración cuando manejamos gran cantidad de datos. El canal de comunicación puede llegar a ser vulnerado debido a que es apetecido por la información que se transmite por este medio, infectándose de tráfico malicioso en redes comunes y a la vez se replica en redes definidas por software afectando en la disponibilidad de la red ya que se saturaría con este tráfico no deseado; por tal motivo la importancia de contar con modelos preventivos en cuanto a seguridad de la información.

Los intrusos de las infraestructuras de red, o como se los conoce como “Hackers” buscan vulnerar estos sistemas y acceder a la información, estas personas se empeñan en encontrar falencias en la seguridad y aprovecharse de las mismas para acceder a datos privados que son críticos para cualquier institución. La duplicidad y la traición forman una parte intrínseca de sus operaciones diarias (Dupont, Côté, Savine, & Décary-Hétu, 2019).

Es por ello la necesidad de aplicar mecanismos de protección a la red definida por software para mejorar los niveles de calidad del servicio y optimizar los niveles de seguridad de la información.

1.2.Objetivos de la Investigación

Garantizar la integridad de la información es primordial en las infraestructuras de red y telecomunicaciones, mediante la implementación de un IDS en una Red definida por software se permite mejorar la identificación del tráfico malicioso.

1.2.1. Objetivo general

Realizar el diseño de un sistema de detección de intrusos a través de redes definidas por software con la finalidad de identificar tráfico malicioso tomando como referencia una arquitectura GPON de un proveedor de servicios.

1.2.2. Objetivos específicos

Revisar la literatura asociada con Redes Definidas por Software, Sistemas de Detección de Intrusos y la tecnología GPON; con el fin de aplicar esta tecnología en redes de telecomunicaciones.

Identificar el tráfico malicioso por medio de un IDS para clasificar los riesgos, en base a los niveles de seguridad que se requiera en una arquitectura GPON.

Diseñar un entorno de simulación controlado por un IDS sobre una red SDN, por medio de máquinas virtuales que permitan generar diferentes flujos de tráfico e identificar el tráfico malicioso.

Evaluar la solución para validar el Sistema de detección de intrusos en una SDN.

1.3.Justificación

Las empresas de Telecomunicaciones por lo general tienen redes de servicios de internet, telefonía móvil, telefonía fija, etc. Y además contienen gran cantidad de información interna y externa (clientes); toda infraestructura se encuentra vulnerable para que hackers informáticos incurran en delitos, si bien es cierto la seguridad debe enmarcarse a nivel de toda la infraestructura tecnológica. El presente proyecto pretende dar un punto de partida en el servicio de detección de intrusos a través de una SDN (Ali Ujjan, Pervez, & Dahal, 2018).

La implementación de un IDS sirve para mejorar la gestión de seguridad de la información independientemente de los riesgos que están identificados, evaluados y gestionados en la organización (Nam & Kim, 2018).

El proyecto busca identificar el tráfico fuera de lo normal sobre una SDN alertando los sistemas de seguridad de la información que se encuentra en la infraestructura de Telecomunicaciones. A nivel global se registran 100 asaltos informáticos por día y Ecuador está en la lista de los más perjudicados (FISCALIA GENERAL DEL ESTADO, 2019), por tal razón se protegerá de diferentes ataques internos y externos. Este proyecto será un aporte significativo para que el área tecnológica mejore sus servicios (Hendrawan, Sukarno, & Arief Nugroho, 2019).

Esta investigación se enmarca en el objetivo 5 del Plan Nacional de Desarrollo 2017-2021, que en su política 5.6 cita: ” Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades” (Plan Nacional de Desarrollo 2017-2021 Toda una Vida, 2017).

Esta investigación corresponde a la línea de investigación Desarrollo, aplicación de software, cyber security, definida por la Universidad Técnica del Norte.

CAPITULO II

MARCO REFERENCIAL

2.1.Antecedentes

La propuesta de este estudio es diseñar un entorno controlado para la detección temprana de intrusos en redes definidas por software SDN, esto permite identificar el tráfico no deseado para tener una visión global de las posibles saturaciones en la red debido a agentes extraños. Las SDN son una próxima generación tecnológica que permiten transformar un sistema físico a uno por software, mejorar parámetros de flexibilidad, gestión simplificada a través de la abstracción de la red y centralizar.

Existen problemas y vulnerabilidades en el entorno de redes tradicionales que se pude filtrar tráfico que no es propio de la red, por lo general son ataques de inundación de paquetes dirigidos. Este papel examina cómo implementar funciones de seguridad de red utilizando Tecnología SDN para estos problemas de seguridad. Por tal motivo la necesidad de una estructura de seguridad de SDN utilizando el software IDS de código abierto existente.

Según Nam & Kim (2018) es importante implementar sistemas de firewall, escaneo de red y detección de tráfico anormal en existentes entornos de red utilizando OpenFlow de SDN. Además, que no es fácil transferir el contenido del paquete al controlador, este autor resuelve el problema con Suricata utilizando el método del reflejo.

Según E Tego, F Matera & V Attanasio (2017) la calidad de servicio en una red óptica es importante ya que este tipo de redes manejan gran cantidad de clientes y de información. Para ello el autor detalla la importancia de tener la Unidad central (orquestador) que administra automáticamente los enlaces GbE en una red regional impulsada por el análisis de rendimiento de la red realizado por dicho plano de mPlanemeasurement utilizando sondas activas y pasivas.

Con la evolución tecnológica, el acceso a internet se masificó al igual que los requerimientos de los usuarios que necesitan un mayor ancho de banda, lo que es un reto para varios ISP que brindan este tipo de servicios (Loayza-Valarezo, Guaña-Moya, & Pumares-Romero, 2020).

2.2.Marco teórico

En la presente sección corresponde a la fundamentación teórica, la misma que enmarca definiciones importantes, las cuales permitirán el correcto desarrollo de la investigación; en general los ítems que se analizará son los siguientes: los sistemas de detección de intrusos, redes definidas por software (SDN) y las arquitecturas GPON.

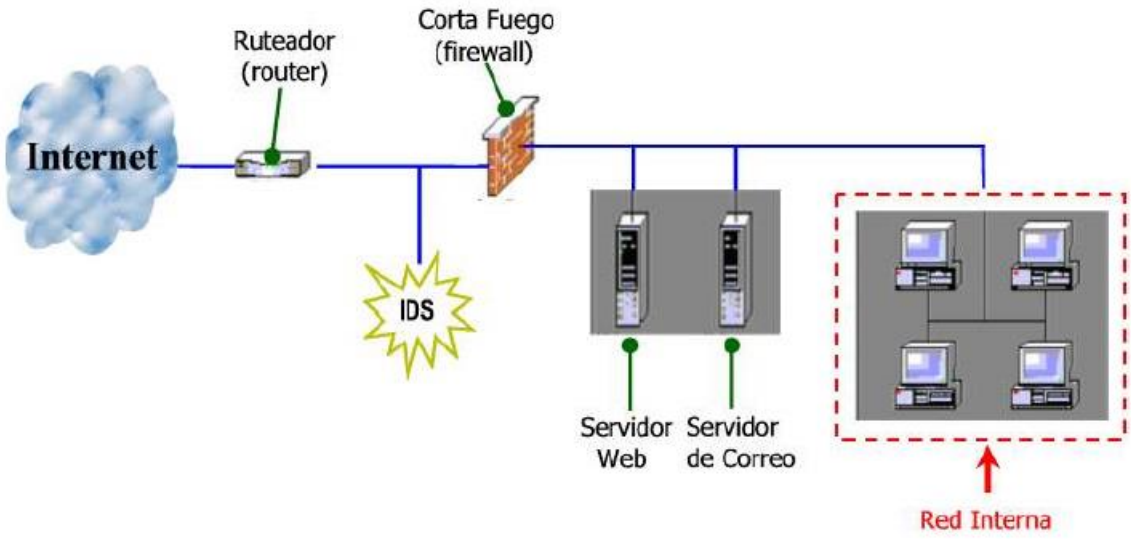
2.2.1. Definición de un Sistema de Detección de Intrusos.

Un sistema de detección de intrusos, o IDS es una herramienta de seguridad cuya finalidad es detectar ataques a los sistemas informáticos. Estos se encargan de recolectar y analizar información con el fin de proporcionar una notificación de un ataque potencial o de uno en curso; en lo cual detecta intrusiones que son acontecimientos transitorios o vulnerabilidades que son exposiciones que pueden llegar a intrusiones o ataques (Salazar Hernández, 2016).

Los IDS tienen diferentes posiciones dentro de las topologías de red, una forma de instalar es colocar en la DMZ (Zona Desmilitarizada) cuyo significado es que mantiene la zona que se muestra al exterior. En la **Figura *1*** se observa la ubicación de un IDS en una red simple y con pocos equipos de red, se debe instalar antes del cortafuego exterior debido a que en este lugar permite reconocer los puertos abiertos y escanear cualquier anomalía (Ocampo, Castro Bermúdez , & Solarte Martinez, 2017).

Figura 1

Red con IDS Simple

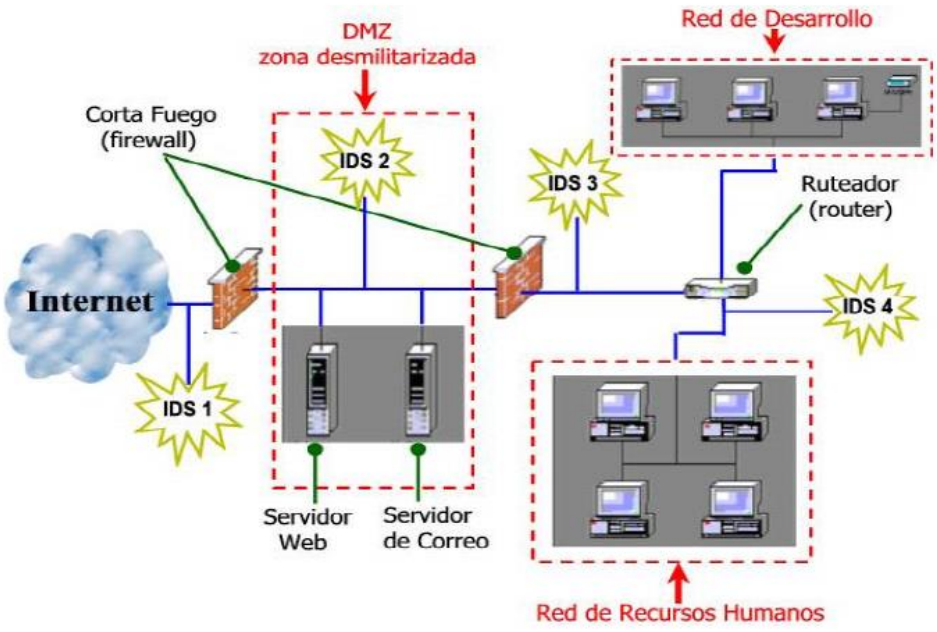


Nota. El gráfico representa una red básica con un IDS. Tomado de (Ocampo, Castro Bermúdez , & Solarte Martinez, 2017).

Cuando se tiene redes grandes, se requiere de varios IDS, en la **Figura *2*** se observa que el IDS1 se emplea para el rastreo de puertos en ambos sentidos ya que detecta y notifica. En el IDS2 se monitorea el tráfico de la DMZ, por otro lado, el IDS3 e IDS4 controlan la red interna mismos que cuentan con sensores que capturan la información, ejecuta cálculos y notifica (Ocampo, Castro Bermúdez , & Solarte Martinez, 2017).

Figura 2

Red Compuesta con varios IDS



Nota. El gráfico representa una red compuesta con varios IDS. Tomado de (Ocampo, Castro Bermúdez , & Solarte Martinez, 2017).

2.2.1.1.Tipos de IDS

Entender un IDS en cuanto a su funcionalidad es primordial al momento de elegir cual se implementará en el sistema de seguridad informático. Existen IDS basados en comportamiento, realizando un seguimiento buscando anomalías en el sistema, algunos son servicios independientes que analizan pasivamente cualquier paquete externo y otros combinan herramientas para mejorar la detección de intrusos (Sanchez Restrepo, 2017).

A continuación, los principales tipos de IDS:

IDS basado en anfitrión (host), analiza diferentes tipos de registros de archivos (kernel, sistema, servidores, red, cortafuegos) con los registros internos que contiene sobre ataques

informáticos conocidos. De la misma manera se puede verificar la integridad de los archivos en base de datos confidenciales creando una suma de verificación de cada archivo de texto plano, comparando periódicamente con el archivo original, en caso de no coincidir alerta al administrador (Sanchez Restrepo, 2017).

Otro tipo de IDS son los sistemas de intrusos basados en red, este escanea los paquetes de red a nivel de enrutador y audita la información de los paquetes. Cada paquete escaneado con su propia base de datos de firmas de ataques asigna un nivel de severidad para cada paquete, de esta manera detecta un alto nivel notificando la anomalía para que se investigue la naturaleza (Sanchez Restrepo, 2017).

2.2.1.2.Herramientas IDS Open Source

Se tiene las siguientes herramientas:

- Snort es un sistema de detección de intrusos de código abierto que funciona mediante la escritura de reglas que detectarían amenazas emergentes. A diferencia de utilizar firmas, las reglas permiten detectar vulnerabilidades reales, es decir especifica características únicas del tráfico de red para luego bloquear o eliminar según se configure.
- Suricata es una herramienta IDS de arquitectura distinta que se comporta de la misma manera que Snort usando las mismas reglas. Al igual que Snort depende de estándares, y a pesar de que ofrece similitud en las reglas, también presenta diferentes cadenas para comparar limites hipotéticos en los sistemas más rápidos.

- Bro funciona de manera diferente ya que busca amenazas específicas y dispara alertas, principalmente se usa para registrar el comportamiento de la red con su propio lenguaje de administración (Bro-Script).
- Kismet sirve como un IDS remoto para redes Wireless el cual analiza ocasiones en los sistemas, es decir puntos de entrada falsos como un Access Point sustituyendo el SSID/MAC de los equipos (Coyla Jarita, 2019).

2.2.1.3.Herramientas IDS Comerciales

En la industria de las Telecomunicaciones se tiene varias empresas dedicadas al desarrollo de herramientas IDS, las mismas que se encargan de tener actualizaciones periódicas que permiten mejorar los sistemas de seguridad de las redes de datos. A continuación, se tiene las siguientes herramientas IDS:

- McAfee Network Security Platform es un Sistema que bloquea los ataques nuevos y desconocidos basado en firmas y sin firmas con soporte para VMware NSX y OpenStack lo que permite la agrupación de seguridad mediante redes físicas y virtuales.
- DefensePro DDoS Pro-IPS se especializa en ataques DDoS es un sistema que detecta y protege este tipo de intrusiones mediante la realización de modelos de seguridad.
- StoneSoft es un producto que brinda servicios de firewall/vpn, IPS. Estos productos son de tecnología única, originalmente desarrollada para Check Point.
- IBM Security Network Intrusion Prevention System bloquea ataques automáticamente preservando el ancho de banda y la disponibilidad. Dispone de una interfaz de administración local basada en la web para efectuar actualizaciones.

- Cisco Sourcefire es un sistema que recibe cada dos horas nuevas políticas, recibiendo periódicamente actualizaciones brindando seguridad a cada producto de seguridad de Cisco. Esto permite la detección temprana de intrusos (Coyla Jarita, 2019).

2.2.1.4. Comparación de herramientas Open Source.

En la **Tabla *1*** se muestra un cuadro comparativo entre las principales herramientas Open Source, en cuanto a las características que se analizan de las herramientas IDS se tiene las siguientes:

- Multi-Hilo: son unidades centrales que soporta múltiples hilos de ejecución.
- Soporte IPV6: es una actualización del protocolo Ipv4, debido al problema de agotamiento de direcciones.
- Opciones de protocolos automáticos: asignación de protocolos predeterminados (DNS, DHCP).
- Aceleración con GPU: se acelera mediante un coprocesador dedicado al procesamiento de gráficos.
- Análisis avanzado de HTTP: permite interfaz gráfica mediante el protocolo HTTP.
- Lenguaje: son medios que permiten la utilización de los IDS.
- Integrable: se puede añadir a otras plataformas.
- Detección de alertas basada en reglas: mediante reglas se determina la ejecución de reglas que funcionan como alerta.
- Detección de alertas mediante scripts: es un mecanismo de ejecutar alarmas, mediante decodificaciones en texto plano.

Tabla 1

Comparación de Herramientas IDS Open Source.

Características	Bro	Snort	Suricata
Multi-hilo	No	Si	Si
Soporte IPv6	Si	Si	Si
Detección automática de protocolos	Si	Si	Si
Aceleración con GPU	No	Si	Si
Análisis Avanzado de HTTP	Si	Si	Si
Tecnologías soportadas	Simuladores	SDN	SDN
Integrable	No	Si	Si
Detección de alertas basada en reglas	No	Si	Si
Detección de alertas basada en scripts	Si	No	No

Nota. En la siguiente tabla se muestra una comparación entre los sistemas IDS.

Según el estudio de Raza Shah & Issac (2018) se evaluó el rendimiento de los sistemas de detección de intrusos, se tiene que Suricata puede procesar una velocidad de tráfico de red mayor que Snort con una menor tasa de caída de paquetes, pero consume mayores recursos computacionales. Snort tuvo menos precisión, obteniendo un número elevado de falsas alarmas positivas. Para resolver este problema, se debe seleccionar el algoritmo de mejor rendimiento para el complemento adaptativo de Snort permitiendo resultados reales en la red de datos.

2.2.2. Redes Definidas por software

Redes definidas por software son redes que tienen la capacidad de inicializar, controlar, cambiar y gestionar el comportamiento del tráfico mediante APIs. SDN separa los planos de control y datos de los dispositivos de red desplazando el plano de control a la unidad centralizada

o controlador SDN que se encarga de definir y comunicar las reglas de reenvío de tráfico a la red SDN.

En SDN se cambia la funcionalidad de los switches, haciendo que solamente se encarguen de reenvío simple de datos para que el NOS (Network Operating Systen) se encargue de la lógica de control, simplificando las políticas, facilidad en la configuración e implementación de nuevos servicios (Pereira & Gamess , 2017).

2.2.2.1.Arquitectura de SDN

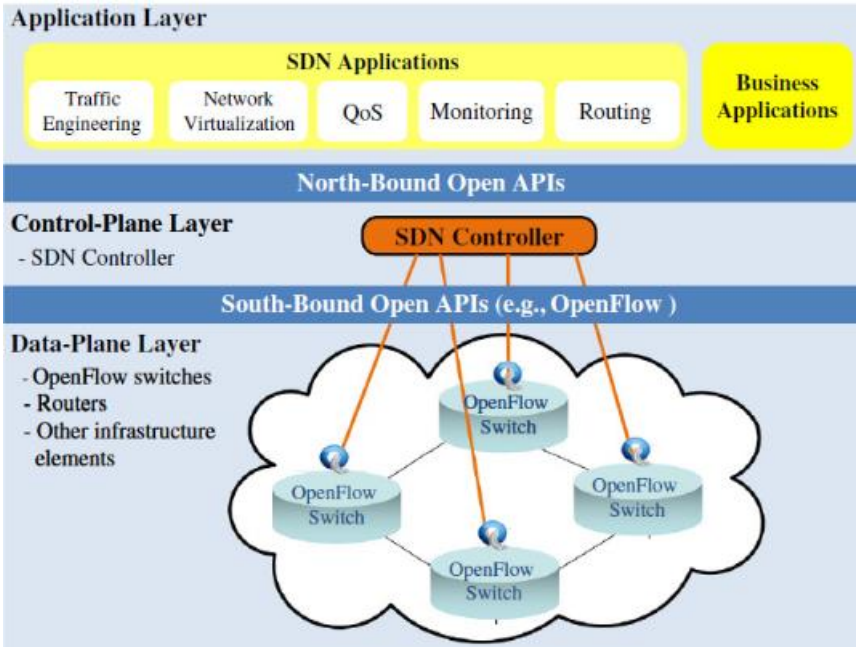
Una SDN está compuesta por las siguientes capas: plano de datos, plano de control y plano de aplicación.

El plano de datos es una capa que controla a través de una interfaz específica de la SDN y es responsable de la transmisión del flujo de datos. El plano de control determina si es de enrutar, reenviar o rechazar flujos de datos a través de aplicaciones y servicios de red. Además, el plano de control transfiere las operaciones del plano de datos a la capa de aplicación en forma de (Application Program Interface) API.

En la **Figura *3*** se muestra como los controladores se comunican con las aplicaciones externas mediante APIs Northbound y Southbound abiertas, infraestructura de red, aplicaciones, hipervisores y virtualización de redes (Pereira & Gamess , 2017).

Figura 3

Arquitectura SDN.



Nota. El gráfico representa la arquitectura lógica de una red SDN. Tomado de (Pereira & Gamess , 2017)

2.2.2.2.Software de Simulación para redes SDN

En esta sección se analizará los principales sistemas de simulación y emulación para redes SDN, a continuación, se detalla una breve reseña de cada uno de estos:

- Estinet es un simulador y emulador de red que se usa en redes de telecomunicaciones, incluye una interfaz gráfica que permite construir y depurar la simulación beneficiando la integración directa de protocolos TCP/IP y UDP/IP de Linux.

- Ns-3 es un simulador con finalidad educativa, esta herramienta es de código abierto y permite la inclusión de otros sistemas, siendo escalable para modular y emular. (Calle, Tovar, Castaño, & Cuéllar, 2018)
- Mininet es la herramienta de emulación de SDN que permite crear redes virtuales, es ideal para emular entornos reales de producción, debido a su compatibilidad con controladores reales (Keti & Askar, 2015).

Estas soluciones permiten desempeñar en muchos campos de la investigación, educación y experimentales; estos sistemas continúan en desarrollo y se tiene grandes expectativas ya que son métodos sencillos que experimentan con OpenFlow y SDN. En la **Tabla 2** se muestra una comparación entre los sistemas de simulación, evaluando las características principales, modo de funcionamiento, compatibilidad, escalabilidad y resultado repetible, este último quiere decir que se obtiene resultados coherentes en varias repeticiones de simulación (Mohammad Mousavi & St-Hilaire, 2015).

Tabla 2

Sistemas de Simulación para SDN

Característica	**ESTINET**	**NS-3**	**MININET**
Modo de simulación	Si	Si	No
Modo de emulación	Si	No	Si
Compatible con controladores reales	Si	No	Si
Resultado repetible	Si	No	Si
Escalabilidad	Alta (para un solo proceso)	Alta (para un solo proceso)	Media (para múltiples procesos)

Nota. En la siguiente tabla se muestra una comparación entre los sistemas de simulación para SDN.

2.2.3. Arquitectura de una Red Gpon FTTH

La tecnología de redes ópticas pasivas (PON) son las más utilizadas en redes de acceso debido a las ventajas que ofrecen, como la alta eficiencia, la seguridad y la reducción de costos. Sin embargo, la gestión de red en PON aún no está automatizada y necesita la intervención del operador de red. Se identifica los beneficios de la red óptica pasiva con capacidad de Gigabit (GPON) se mejora la gestión del tráfico al mismo nivel que un conmutador SDN. Es decir, la infraestructura física de GPON funcionará en un conmutador SDN virtual habilitado OpenFlow (W. Lee, Li, & Wu).

Una red pasiva óptica (PON) se complementa con los sistemas de acceso FTTx, en este caso se especificará en los que son redes hacia el hogar, es decir Fiber to the home (FTTH).

A continuación, se tiene las Topologías PON.

- Topología tipo árbol.
- Topología tipo bus.
- Topología tipo anillo.

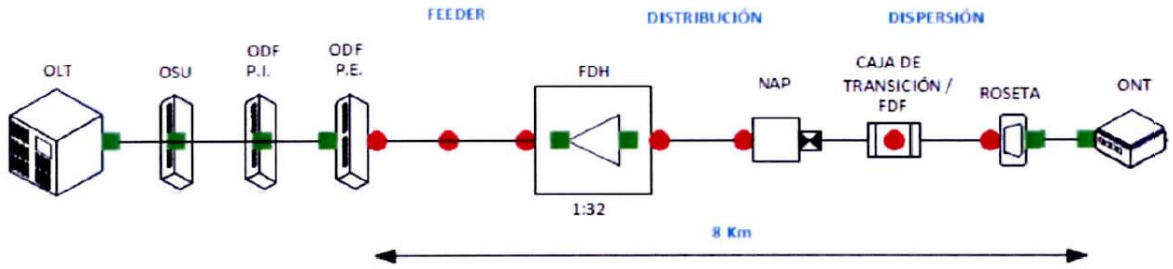
La red GPON está compuesta por:

- OLT: Equipo que gestiona el tráfico desde el uplink MPLS con los equipos terminales. Niveles de splitteo 1/32 y 1/64
- ONT: Equipos terminales de cliente.
- ODN: La red de Fibra Óptica más splitters.

Existen dos formas de construcción en arquitecturas GPON una de ella es Centralizada como se puede mostrar en la **Figura *4***, esta consiste en realizar una sola división de luz (CNT EP, 2017).

Figura 4

Arquitectura GPON Centralizada

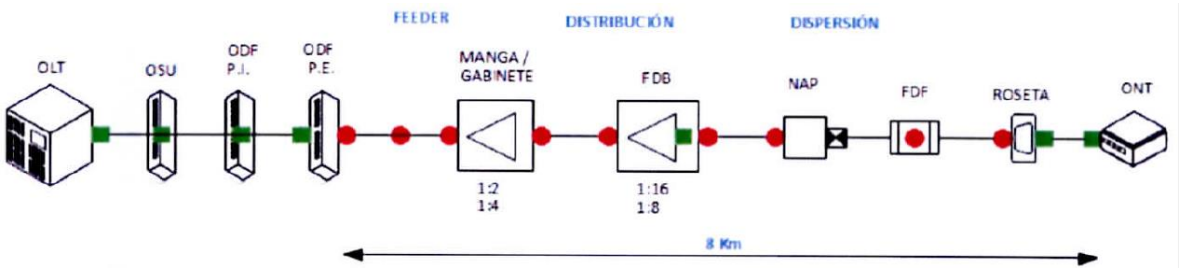


Nota. El gráfico representa la red óptica pasiva centralizada en tres etapas. Tomado de la Normativa Técnica de la Corporación Nacional de Telecomunicaciones CNT EP (2017).

Según la normativa técnica de construcción de la CNT EP (2017) tenemos otro tipo de construcción de redes GPON, que es la arquitectura Tipo Cascada, esta consiste en tener dos niveles de espliteo, lo que permite una mejor escalabilidad con respecto a la centralizada como se puede mostrar en la **Figura *5***.

Figura 5

Arquitectura GPON Tipo Cascada.



Nota. El gráfico representa la red óptica pasiva tipo cascada en tres etapas. Tomado de la Normativa Técnica de la Corporación Nacional de Telecomunicaciones CNT EP (2017).

2.2.3.1.Evolución de las redes PON

En cuanto a la regulación se tiene dos instituciones que norman las redes PON:

- ITU-T (International Telecommunications Union)
- IEEE.802 (Institute of Electrical and Electronic Engineers)

A continuación, en la **Tabla *3*** se observa las características principales de las normativas de regulación de las redes PON, se tiene el tipo de tecnología, la distancia de las redes de distribución OLT-CLIENTE, tecnología de acceso y velocidades de transmisión de datos.

Tabla 3

Regulación de Redes PON

Normativa	Año	Tecnología	Distancia	Velocidad DS	Velocidad US	Tecnología de acceso
ITU-T G.984.5	2007	GPON2	20KM	2.50 Gbps	2.50 Gbps	TDMA
IEEE 802.3	2005	GEPON	20KM	1 Gbps	1 Gbps	WDM

Nota. En la siguiente tabla se muestra una comparación entre las normativas existentes en arquitecturas GPON. Tomado de Valarezo, Guaña y Pumares (Valarezo, Moya, & Romero, 2019).

2.2.3.2.Vulnerabilidades en Arquitectura GPON

Dentro de la seguridad abarcan algunos conceptos importantes en los cuales podemos definir algunos de ellos que se encuentran involucrados en el desarrollo de este trabajo (Cervantes, Pesantez, Rosales, & Aranda, 2011).

- Amenaza. - Es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto período de tiempo en un sitio dado.
- Vulnerabilidad. - Es el grado de pérdida de un elemento o grupo de elementos de bajo riesgo resultado de la probable ocurrencia de un suceso desastroso, expresada en una escala desde 0 (sin daño) a 1 (pérdida total).
- Riesgo. - Es el grado de pérdidas esperadas debido a la ocurrencia de un suceso particular y como una función de la amenaza y la vulnerabilidad (Cervantes, Pesantez, Rosales, & Aranda, 2011).

Las arquitecturas GPON no se encuentran exentas de ataques que intenten alterar la disponibilidad de este servicio, existen vulnerabilidades físicas y lógicas. Las vulnerabilidades físicas en las redes GPON, se deben a malas prácticas constructivas que son susceptibles a que agentes externos e involuntarios causen problemas como roturas del cable de fibra óptica; por otro lado las vulnerabilidades que involucran personas malintencionadas mediante la intercepción de la información que viaja a través de la infraestructura GPON, un ejemplo de un ataque a una red GPON es utilizando un divisor de escuchas a cierta distancia de la OLT y un amplificador de señal permitiendo la intercepción de la luz que viaja por el cable de fibra óptica (M Diaa, 2018).

Las vulnerabilidades lógicas se pueden desarrollar mediante ataques DDoS a las interfaces de red, este tipo de ataque cibernético busca saturar los puertos e interfaces con peticiones de varios dispositivos logrando colapsar las redes; otro ataque puede ser de suplantación de identidad de equipos GPON en redes inalámbricas de usuarios finales que son una puerta de entrada hacia la Infraestructura interna de red del proveedor (M Diaa, 2018).

La arquitectura GPON tiene ciertas vulnerabilidades en las capas de red, transporte y aplicación, por defecto tienen la vulnerabilidad de inundación y robo de ancho de banda debido al exceso de consumo de los usuarios, inyección de virus, troyanos spyware, de igual manera ataques de Hijacking o secuestro de identidad del usuario, son muchos los escenarios que se puedan dar en este tipo de redes (Cervantes, Pesantez, Rosales, & Aranda, 2011).

2.2.4. IDS en Redes SDN

La arquitectura de una SDN tiene gran potencial de innovación en las NGN (Redes de nueva generación), esto debe ir de la mano de la seguridad de las tecnologías, esto se respalda con la integración de inteligencia en los IDS existentes haciendo un análisis en la reprogramación centralizada (Skowyra, Bahargam, & Azer, 2016).

Los IDS son esenciales para proteger a las infraestructuras de red de posibles ataques, y son soluciones de SDN. Según los autores Skowyra, Bahargam & Azer (2016) propone un aprendizaje de IDS que utiliza SDN en dispositivos móviles integrados, son nuevas tendencias de seguridad que se puede realizar en conjunto con estas dos tecnologías.

Estos sistemas analizan contenidos de la trama para buscar si hay un patrón de ataque, por lo que el contenido del paquete en el plano de datos debe transferirse a la SDN. Sin embargo, en

el protocolo OpenFlow permite transferir los datos del controlador, por lo que la implementación de IDS no es fácil (Nam & Kim, 2018).

Uno de los métodos implementados en sistemas IDS, de acuerdo con la investigación de Nam & Kim (2018) , es conocido como reflejo, que consiste en la copia de todos los paquetes que pasan por el equipo de red y transferirlos a un servidor específico. Este método también es ampliamente utilizado en los sistemas de detección de intrusos de red existentes que no usan la tecnología SDN, los paquetes reflejados son los ataques. Este método permite identificar si el paquete es malicioso o es un tráfico normal de navegación.

2.2.5. Metodología Offensive Security

La metodología OFFENSIVE SECURITY permite ejecutarse en plataformas reales, lo que le hace óptimo para ser implementado en una arquitectura GPON que se encuentra en producción en un proveedor de servicios de Internet, permitiendo validar las soluciones propuestas por el auditor.

Según (Misaza, 2013) define a esta metodología principalmente en la rama de Ethical Hacking, una herramienta a nivel mundial que permite realizar pruebas de intrusión y estudios sobre la seguridad informática. La principal función es estudiar la seguridad ofensiva para explotar las vulnerabilidades. A continuación, las fases de la metodología:

Recolección de la información. En esta primera fase se hace un barrido de datos en este caso, todo lo referente al ISP víctima.

Análisis de vulnerabilidades. Se continua con el proceso teniendo en cuenta el paso anterior para encontrar debilidades en todos los datos encontrados, de esta manera facilitar la vulneración de los sistemas.

Definición de objetivos secundarios. En este punto se evidencia vulnerabilidades de los sistemas, lo que permite determinar los primeros objetivos para evaluar.

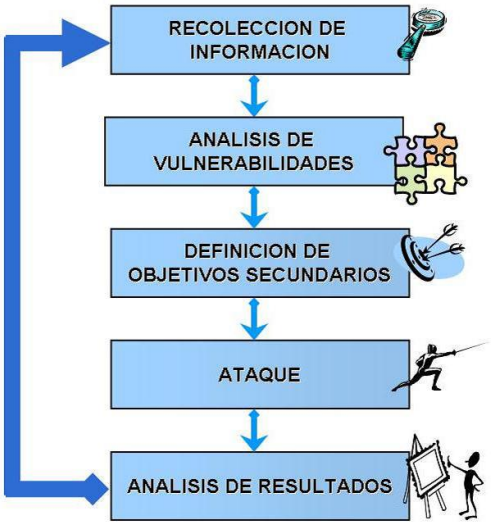
Ataques. Una vez se tenga los objetivos se procede a las pruebas de intrusión, con herramientas de auditoria informática.

Análisis de resultados. Por último, se recopila todos los resultados para determinar las soluciones respectivas.

Lo ideal de esta metodología es una vez terminado las fases, se debe solucionar los problemas encontrados y realizar una vez más el test de penetración y así validar los resultados obtenidos y dar una solución real a un entorno de producción que se encuentra en funcionamiento con usuarios que noten la mejora de su servicio.

Figura 6

Metodologia Offensive Security



Nota. En la presente ilustración se observa las fases de la Metodología Offensive Security. Tomado del sitio web (Isaza, 2013).

2.2.6. ISO 27005

La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información. Es compatible con los conceptos generales especificados en la norma ISO 27001 y se encuentra diseñada como soporte para aplicar de forma satisfactoria un SGSI basado en el enfoque de gestión de riesgo (ISO, 2018). La norma cuenta con los siguientes pasos:

- Establecimiento del contexto
- Identificación del riesgo
- Estimación del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo

Se define criterios de evaluación de impacto, con la finalidad de identificar el efecto del riesgo para los objetivos, por lo general se consideran las siguientes variables:

- Reputación / confianza
- Financiero
- Productividad

De la misma manera se analiza criterios de evaluación:

- Alto impacto (valor de impacto =3)

- Medio impacto (valor de impacto=2)
- Bajo impacto (valor de impacto=1)

Cuando se evalúa las áreas de seguridad, se procede a determinar un color para representar, los criterios de evaluación por color son los siguientes:

- **Verde**. El área está haciendo todo bien. No se necesita ninguna mejora.
- **Amarillo.** El área está haciendo algunas actividades bien, hay espacio para la mejora.
- **Rojo.** El área no está haciendo las actividades bien. Se debe mejorar muchas actividades (Espinosa , Martínez, & Siler, 2014).

2.3.Marco legal

En esta sección se tiene todo lo referente a la documentación legal que se requiere en la investigación, aspectos importantes sobre legislación de delitos informáticos, leyes vigentes en el Ecuador.

2.3.1. Ley Orgánica de las Telecomunicaciones

La Ley Orgánica de Telecomunicaciones. (LOT). Es un organismo cuyo objeto es desarrollar, el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado.

Artículo 13.- Redes privadas de telecomunicaciones.

Las redes privadas son aquellas utilizadas por personas naturales o jurídicas en su exclusivo beneficio, con el propósito de conectar distintas instalaciones de su propiedad o bajo su control. Su operación requiere de un registro realizado pante la Agencia de Regulación y Control

de las Telecomunicaciones y en caso de requerir de uso de frecuencias del espectro radioeléctrico, del título habilitante respectivo.

Artículo 20.- Obligaciones y Limitaciones.

La Agencia de Regulación y Control de las Telecomunicaciones, determinará las obligaciones específicas para garantizar la calidad y expansión de los servicios de telecomunicaciones, así como su prestación de condiciones preferenciales para garantizar el acceso igualitario o establecer limitaciones requeridas para la satisfacción del interés público, todo lo cual será de obligatorio cumplimiento.

Artículo 22.- Derechos de los abonados, clientes y usuarios.

Los abonados, clientes y usuarios de servicios de telecomunicaciones tendrán derechos:

- A la privacidad y protección de sus datos personales, por parte del prestador con el que contrate servicios, con sujeción al ordenamiento jurídico vigente.

Artículo 76.- Medidas técnicas de seguridad e invulnerabilidad.

Las y los prestadores de servicios ya sea que usen red propia o de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente.

Artículo 77.- Interceptaciones.

Únicamente se podrán realizar interceptaciones cuando exista orden expresa de la o el Juez competente, en el marco de la investigación de un delito o por razones de seguridad pública y del Estado, de conformidad con lo que establece la ley y siguiendo el debido proceso.

Artículo 78.- Derecho a la intimidad.

Para la plena vigencia del derecho a la intimidad establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal.

Artículo 85.- Obligaciones adicionales.

La Agencia de Regulación y Control de las Telecomunicaciones establecerá y reglamentara los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios con el fin que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios (Barrezueta, 2015).

2.3.2. COIP

El Código Penal es un instrumento del Estado para sancionar o imponer penas a quienes se hallaron culpables en la materialización de un delito tipificado en la ley, el antiguo código ha sido modificado por varias leyes entre las que constan la ley de comercio electrónico, firmas electrónicas y mensajes de datos publicada en el Registro Oficial Suplemento No. 577 de 17 de abril de 2002.

“Artículo 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca,

difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años".

"Artículo 234.- Acceso no consentido a un sistema informático, telemático, o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años" (COIP, 2018).

CAPITULO III

MARCO METODOLÓGICO

El presente proyecto se realizará mediante la identificación de tráfico malicioso, en un entorno de emulación para posterior realizar pruebas en un entorno real, en una infraestructura GPON, clasificando los datos según el riesgo que se presente en la infraestructura, se adoptará el sistema de colores que clasifica la gestión de riesgos de la ISO 27005. Sin embargo, se implementará un sistema de detección de intrusos el mismo que estará en un entorno virtual de redes definidas por software.

3.1.Descripción del área de estudio

La investigación se ejecutará mediante un entorno real de cualquier tipo de infraestructura de red, para la toma de datos. La implementación de un IDS es un aporte importante en las redes de datos, que tiene la finalidad de identificar información fuera de lo común, la misma que es crucial para garantizar un servicio de calidad hacia los usuarios de cualquier sistema informático, evitando saturaciones.

3.2.Enfoque y tipo de investigación

Para la siguiente investigación se adoptó un método mixto, ya que implica la recolección de datos cuantitativos y cualitativos. Se tiene el método cuantitativo del estudio para contabilizar por medio de datos estadísticos como es la clasificación de datos según su riesgo y el método cualitativo es para comparar las características de los sistemas que mejor se adapten a lo que se tiene como objetivo de estudio.

Para este estudio se debe analizar criterios en base a datos obtenidos en la emulación; se pretende recolectar datos dónde se tienen dos variables el tráfico normal y el tráfico malicioso las

mismas que no están correlacionadas, esto significa analizar si existe un aumento o disminución de cada variable. Abarcando la recolección de datos y así evaluar lo obtenido.

Se aborda el problema de investigación cuantitativo, debido a que se debe hacer un análisis matemático de los problemas y con estos cuantificar y determinar el riesgo actual y futuro que se tiene en la infraestructura de red GPON.

Esto se determinará con una herramienta que determine el análisis de riesgo que tiene la empresa, para ello se utiliza la norma ISO 27005.

3.3.Procedimiento de investigación

Las variables en esta investigación se determinan según los análisis de tráfico en la infraestructura GPON, complementando el estudio con la norma ISO 27005, la cual permite la clasificación del riesgo que tenga, acorde a los datos identificados por el IDS. Por último, se realizará pruebas de inyección de tráfico malicioso dentro de la red SDN para validar la clasificación de datos según el nivel de seguridad.

3.4.Consideraciones bioéticas

Esta investigación pretende resaltar los riesgos que se tiene al inundarse de tráfico erróneo en las redes SDN, este estudio será beneficioso para todos los usuarios de cualquier tipo de red de comunicaciones, ya que les permitirá una mejor visión del flujo de datos por medio de un detector de intrusos el mismo que identificará y clasificará todo el tráfico que llega a cualquier infraestructura de red. Se requiere modificar los entornos tradicionales utilizando sistemas definidos por software como base para la implementación de un IDS.

La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información.

Es compatible con los conceptos generales especificados en la norma ISO 27001 y se encuentra diseñada como soporte para aplicar de forma satisfactoria un SGSI basado en el enfoque de gestión de riesgo.

3.5.Requerimientos para el análisis de tráfico de la red GPON

En esta parte se tiene que analizar los requerimientos para el desarrollo del estudio en un ambiente de simulación para las respectivas pruebas previo al diseño, para ello se analiza tanto el software y hardware necesario para realizar el estudio del tráfico actual d la red GPON, para luego aplicar la metodología Offensive Security como guía ya que interviene lineamientos de seguridad informática, adicional determinar los niveles de riesgo en base a la normativa ISO 27005.

3.5.1. Software

-NMAP es un sistema de código abierto cuya finalidad es el rastreo de puertos, es importante escanear los puertos abiertos de las redes, ya que sirve para detectar vulnerabilidades en los sistemas de telecomunicaciones.

- SNORT es un IDS que brinda el Servicio de Detección de intrusos, que permite la detección de accesos no autorizados en las redes de datos, para este caso de estudio se requiere la utilización del software SNORT el cual detectará el tráfico malicioso en las redes GPON. SNORT tiene tres usos principales: como rastreador de paquetes como tcpdump, como registrador de paquetes, que es útil para la depuración del tráfico de red, o puede usarse como un sistema de prevención de intrusiones en la red en toda regla.

- La herramienta Kali Linux es fundamental para la auditoria de seguridad en la red GPON, la cual nos permite explotar las vulnerabilidades de los sistemas y realizar los ataques de Intrusión.

- GNS3 es un simulador de redes que permite diseñar topologías de red complejas, en este caso se requiere combinar varios dispositivos en la topología a evaluar lo que hace que este sistema sea óptimo para las pruebas de tráfico malicioso.

3.5.2. Hardware

- Se requiere un computador mínimo con 16Gb de Ram que soporte los sistemas necesarios para realizar la simulación y las pruebas para el análisis de tráfico malicioso.

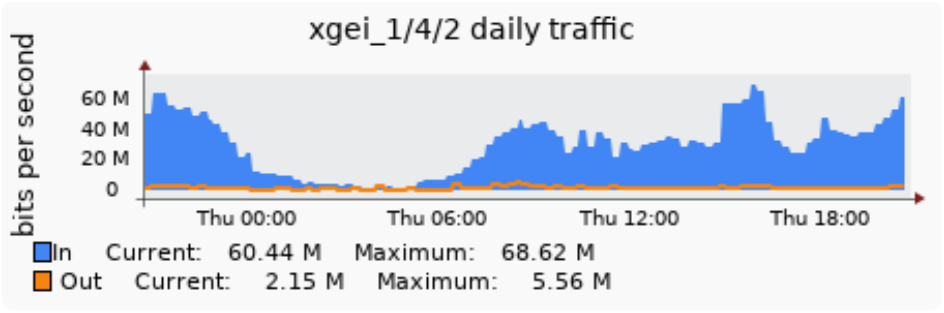
3.6.Análisis de tráfico en redes GPON.

En el ISP tiene como equipo activo principal de la red GPON a la OLT la misma que tiene un sistema de gestión SMARTOLT, el cual permite la activación de los clientes, limitaciones de ancho de banda, habilitación de tarjetas de puertos PON y análisis de tráfico.

Para este caso de estudio se debe analizar el tráfico normal que se tiene, en una de las tarjetas PON, la cual cuenta con 29 clientes activos, en la Figura 7 se muestra el análisis de tráfico normal de los clientes, durante un día.

Figura 7

Análisis de tráfico tarjeta 2 de la OLT

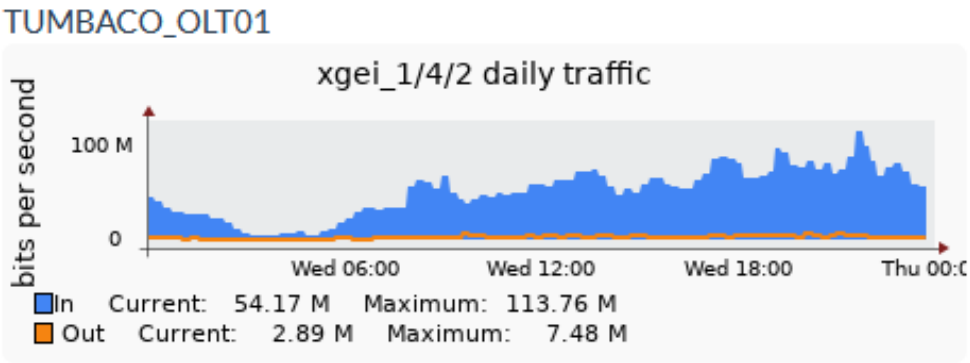


Nota. En la presente ilustración se observa las gráficas de consumo de los clientes conectados en la tarjeta 2 de la OLT del sistema SMARTOLT.

Incrementando usuarios se tiene un incremento exponencial de consumo de Internet por parte de los clientes conectados en la misma tarjeta, ahora se analiza con la cantidad de 49 clientes en la tarjeta 2 de la OLT, esto se visualiza en la Figura 8.

Figura 8

Aumento de consumo en la tarjeta 2

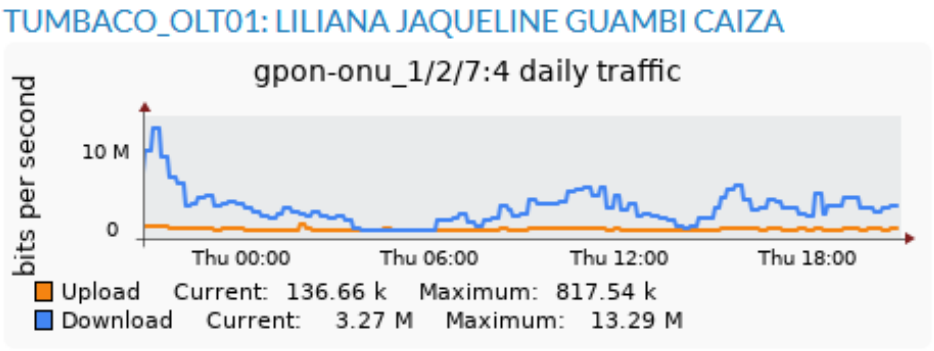


Nota. En la presente ilustración se observa las gráficas del aumento de consumo de los clientes conectados en la tarjeta 2 de la OLT del sistema SMARTOLT.

De la misma manera podemos registrar el consumo por cliente, el cual nos permite realizar un análisis de lo que normalmente consume un abonado en su hogar, local comercial o negocio. En la Figura 9 se tiene una muestra del consumo normal de la cliente Liliana Guambi.

Figura 9

Consumo cliente Liliana Guambi

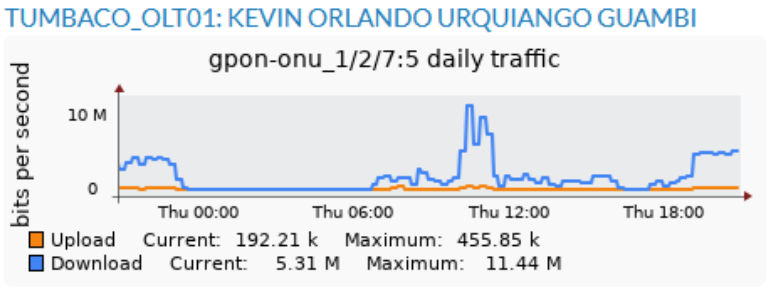


Nota. En la presente ilustración se observa las gráficas de consumo de la cliente Liliana Guambi.

A continuación, en la Figura 10 se tiene el consumo normal de un cliente en un hogar de aproximadamente cuatro personas, se determina este análisis para observar el comportamiento de la red GPON desde sus clientes.

Figura 10

Consumo del cliente Kevin Urquiango



Nota. En la presente ilustración se observa las gráficas de consumo del cliente Kevin Urquiango.

Se tiene como resultado que los usuarios consumen mucho más tráfico Download que Upload; además se puede determinar el tráfico promedio como se visualiza en la siguiente tabla. Cada uno de los clientes consume alrededor de 3 Megas en carga y 300k en descarga, en horas pico el mayor consumo es de 11.44M y 455.85k respectivamente.

Tabla 4

Análisis de tráfico de red

Cantidad de clientes	Consumo Download	Consumo Upnload
1	11.44M	455.85k
29	68.62M	5.56M
49	113.76M	7.48M

Nota. En la siguiente tabla se muestra el análisis de tráfico normal de la red GPON.

3.7.Implementación de la Metodología Offensive Security.

Esta metodología de seguridad informática se puede aplicar en entornos reales, lo cual se analiza una topología en producción con tráfico normal de clientes de un ISP, permitiendo una

solución aplicable a la industria de empresas dedicadas a proveer servicios de Internet a los clientes finales. Esta metodología fue explicada en el capítulo 2 del Marco Referencial de la fundamentación teórica.

3.7.1. Recolección de la información.

En la primera fase se tiene dos opciones, la primera que se conoce a ciegas, es decir no se tiene información de la red y la otra con información, la cual el administrador de la red otorga información valiosa.

A ciegas

En este punto se considera que el intruso no tiene ninguna información de la víctima, para esto se tiene herramientas que permitan investigar datos importantes requeridos para la intrusión en las redes informáticas de la empresa.

Figura 11

Búsqueda en Google, empresa SITEC

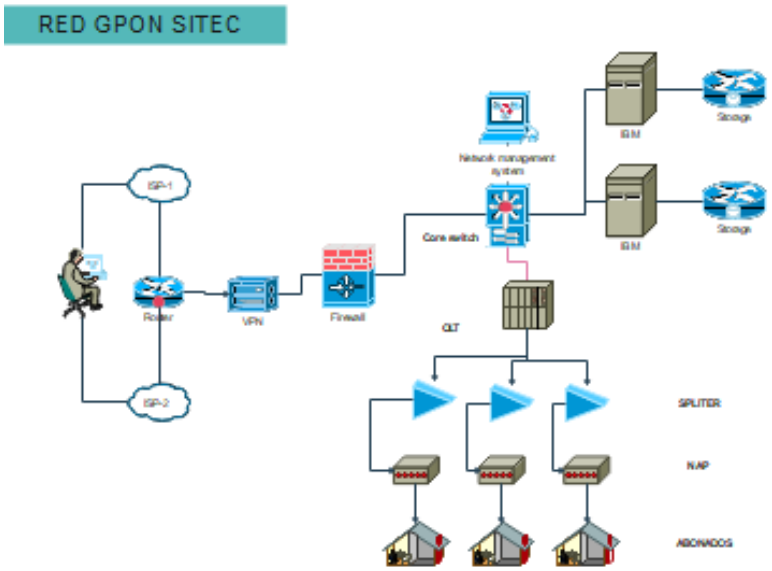
Nota. En la presente ilustración se observa una búsqueda en Google, con la finalidad de encontrar información de la empresa SITEC.

Con información

A continuación, el administrador proporciona la topología de la red, la misma que sirve para proceder con la aplicación de la metodología. Desde el punto de vista de información entregada para una auditoria de seguridad.

Figura 12

Topología de la red GPON de SITEC



Nota. En la presente ilustración se observa la topología de la red GPON de la empresa SITEC.

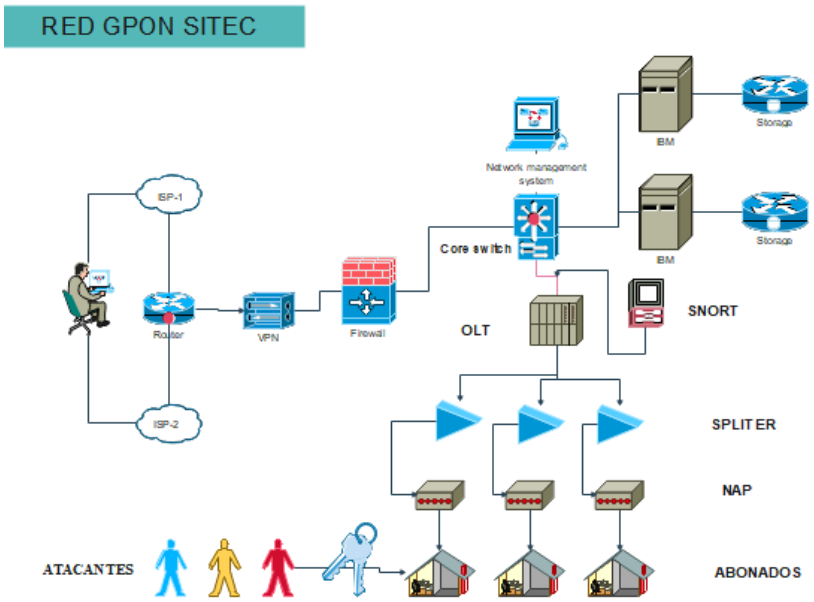
Una vez identificado la topología de red, se debe identificar al atacante; a simple vista este debe estar en el lado del abonado ya que se pretende identificar tráfico malicioso. Para esta prueba se termina los siguientes puntos.

Atacante. – El intruso de la red se ubicará en la casa del abonado, el mismo que estará conectado en la ONU. Para esto se va a instalar el sistema de auditoria informática Kali Linux el mismo que va a estar instalado en el computador del atacante, para enviar tráfico malicioso en la red GPON de SITEC.

IDS Snort. - El sistema de detección de intrusos debe estar conectado a la interfaz de salida del router core y la interfaz de entrada de la OLT, esta conexión será un filtro para poder analizar todo el tráfico que pasa por la red GPON de la infraestructura de red de la empresa SITEC.

Figura 13

Topología de red para el análisis de tráfico malicioso



Nota. En la presente ilustración se observa la topología de la red GPON de la empresa SITEC, con atacantes para analizar el tráfico malicioso.

Situación Actual Software

- Se requiere de un sistema de Gestión para el registro de los clientes de una red GPON, para este caso de estudio se tiene implementado el sistema WispHub, el cual tiene como finalidad llevar un registro de clientes, facturación electrónica, activación de clientes y asignación de direcciones IP para cada uno de los abonados.

- El sistema SMART OLT se encarga del monitoreo de los clientes, el mismo que tiene una interfaz gráfica que permite visualizar cortes y fallos en cuanto a las instalaciones, además de analizar el consumo de tráfico por cliente, tarjeta PON o por la OLT.

Situación Actual Hardware

- Se requiere de una red GPON constituida por equipos activos, los cuales se conforman por la OLT en la central, y las ONTs equipos terminales en los abonados; adicional los equipos pasivos conformados por cables de fibra óptica, mangas para el primer nivel de spliteo y cajas de distribución NAPs con su segundo nivel de spliteo.

- Es necesario la adquisición de un equipo router core, cuya función es el encaminamiento del tráfico de los proveedores de Internet hacia el equipo activo OLT el cual se encarga de enviar los datos a través de la red GPON.

- Servidor DNS, es necesario la adquisición de un servidor físico DNS ya que permite la traducción de dominios en la navegación de los abonados.

- Equipos de borde, son los routers core entregados por los proveedores de Internet, es el punto de conexión entre el proveedor de servicios de Internet y la empresa SITEC cuyo objetivo es brindar el servicio de Internet a los clientes finales.

3.7.2. Análisis de Vulnerabilidades.

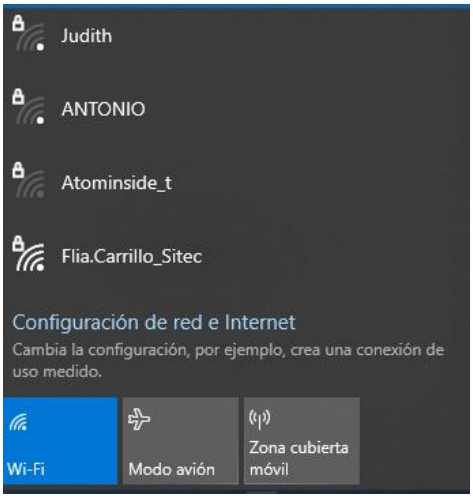
Esta fase consiste en determinar problemas de seguridad en los objetivos determinados en la primera fase. Para esta etapa es posible utilizar herramientas propias del computador de cualquier abonado dentro de la red GPON, esto depende de la organización.

Búsqueda de redes inalámbricas.

La red inalámbrica de los abonados tiene vulnerabilidades las cuales se pueden explotar, para poder ingresar a la red interna de la infraestructura GPON. Se escanea las redes wifi que tengan el SSID con los nombres de la empresa victima a la cual se va a probar la seguridad de estas redes inalámbricas, desde ataques externos de la central.

Figura 14

Red Wifi Víctima



Nota. En la presente ilustración se observa la red wifi de la víctima la cual será la primera puerta de entrada hacia la red de SITEC.

Conexiones Ethernet.

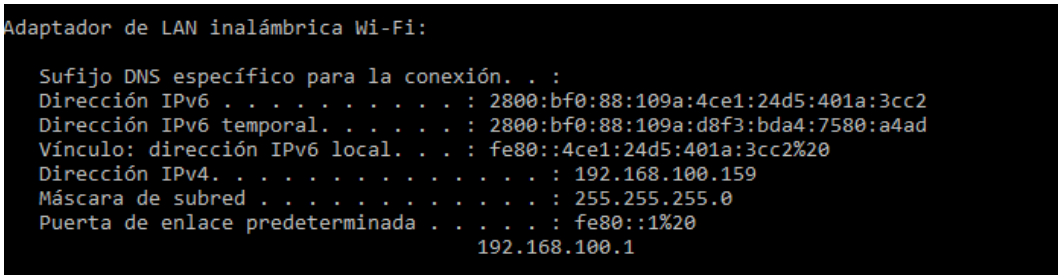
En el otro caso, si el atacante tiene acceso físico, es decir por medio de una conexión cableada por cable UTP hacia la ONT del cliente o abonado. Esto siempre y cuando el atacante busque la manera de acceder al domicilio de un usuario.

Determinar la Ip privada de la red local del abonado.

Para esto se ayuda con el comando ipconfig, que se ejecuta dentro del cmd del computador conectado a la red privada del ISP. En la Figura 13 se tiene la red LAN del cliente, con esto se determina, una dirección de acceso a la ONT, una vez adentro ingresamos con las claves de defecto de la marca Huawei y encontramos el direccionamiento de la WAN, es decir las IPs de la red de los clientes.

Figura 15

Escaneo de la dirección privada de la red



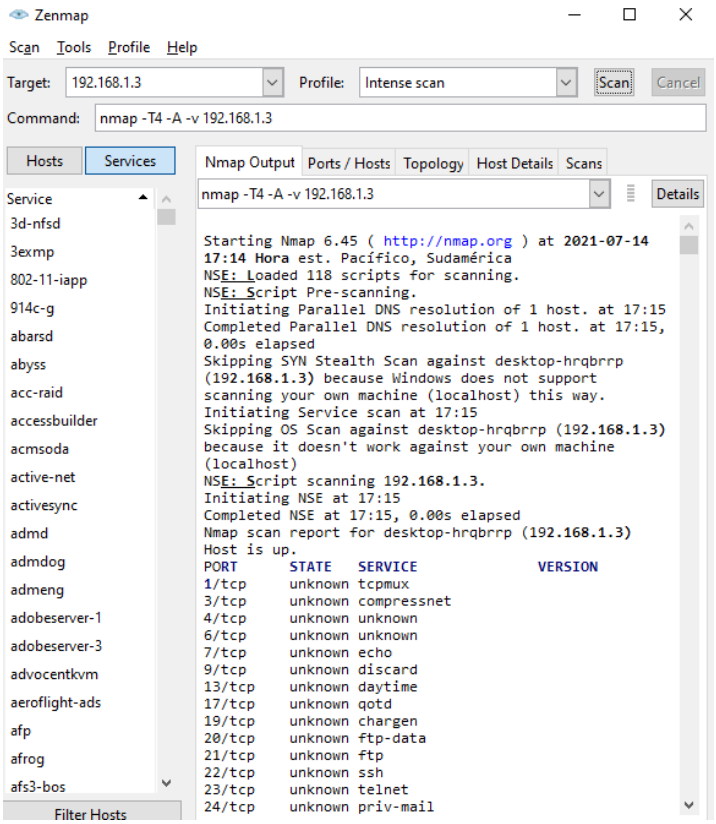
Nota. En la presente ilustración se observa el direccionamiento de la red privada de la víctima la cual se encuentra en la red interna de SITEC.

3.7.2.1.Escaneo de puertos de la ONT.

Este procedimiento es necesario e importante ya que podemos visualizar los puertos abiertos, que sirven como puertas de entrada de los atacantes.

Figura 16

Escaneo de Puertos en la red interna de SITEC



Nota. En la presente ilustración se observa los puertos abiertos de la red interna de SITEC.

3.7.3. Definición de Objetivos.

En esta fase se determina los sistemas victima que se pretende vulnerar, para esto se analiza las fases anteriores.

Objetivos Específicos.

- El consumo normal de navegación de los clientes se tiene como referente en un análisis previo, el ataque directo viene ser hacia la OLT, el cual es un nivel alto en

cuanto al riesgo ya que este equipo activo de la red GPON es el que contiene la información necesaria para la activación de todos los abonados.

- Ataques al servidor DNS donde se hace la traducción de los dominios para la salida al Internet de los clientes.
- El router core en la central de la empresa es vulnerable ya que se realiza la gestión directa de toda la red GPON.
- Un ataque directo a uno de los usuarios de la empresa SITEC, podría clonar o dar de baja al servicio.

Objetivos Secundarios.

- La red inalámbrica de los clientes es vulnerable ya que por ser una red doméstica no cuenta con altos estándares de seguridad, lo que hace un blanco fácil para los atacantes.
- La red cableada de los clientes es un posible objetivo de intrusiones, si el atacante ingresara a un domicilio puede tener acceso mediante un cable ethernet hacia la ONU y de ahí realizar ataques

3.7.4. Ataque.

En esta fase se explota las vulnerabilidades encontradas en los sistemas, para que en la siguiete fase se busque solucionar dichos problemas de seguidad en caso de haberlos.

3.7.4.1.Ataques Lógicos.

En este punto se debe explotar todas las vulnerabilidades encontradas, para estos se tiene los siguientes ataques a la red GPON:

Inundación de tráfico: este ataque consiste en enviar cadenas de datos con el objetivo de saturar las interfaces, hasta el punto de dar de baja a peticiones válidas.

Acorde al autor (Zapata Molina. 2012), son ataques que provocan que un servicio, equipo o recurso sea inaccesible para usuarios legítimos. Para esto se envía mensajes TCP de petición de conexión por parte del cliente, pero sin enviar su confirmación lo cual provoca colapsos en equipos y consumo de recursos en forma desproporcionada, muchas veces la dirección de origen es falsificada.

Suplantación de identidad: En este ataque se pretende suplantar una ONT valida, por una de un atacante.

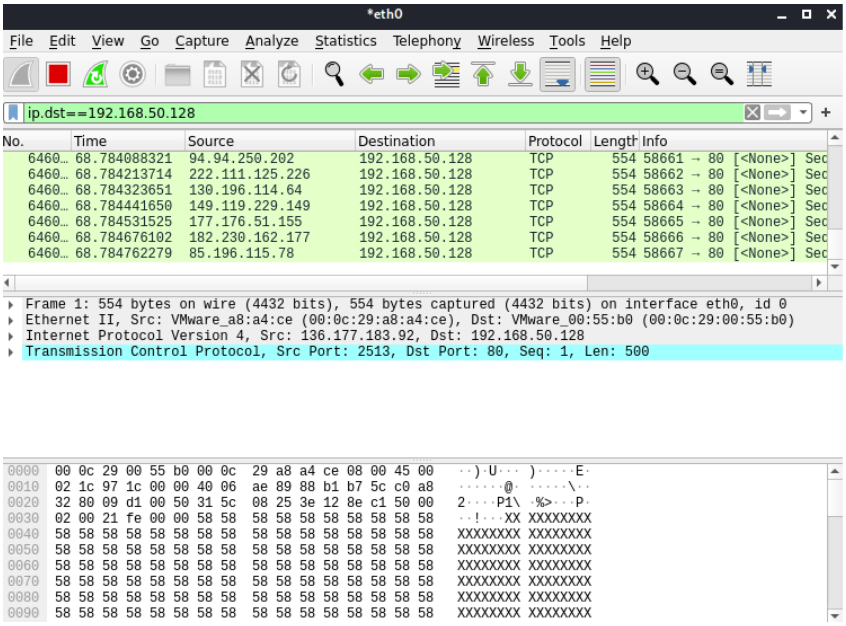
DDoS al router core: Este ataque pretende suspender al equipo principal de la red, lo que es de sumo riesgo ya que de ahí se maneja todo el sistema de los clientes. Cuando se tiene la dirección IP de la víctima podemos hacer un ataque directo para denegar el servicio, para este caso de estudio se realiza el ataque HPING3.

Hping3 –rand-source -d 500 192.168.50.128 -p 80 –faster HPING 192.168.50.128 (eth0 192.168.50.128): NO FLAGS are set, 40 headers + 500 data bytes

El equipo router core tiene habilitado el puerto 80 para el ingreso por medio web, con este ataque se pretende dar de baja el ingreso por este medio, se tiene como resultado un análisis de tráfico por medio de wireshark como se inunda de peticiones falsas.

Figura 17

Análisis de tráfico malicioso

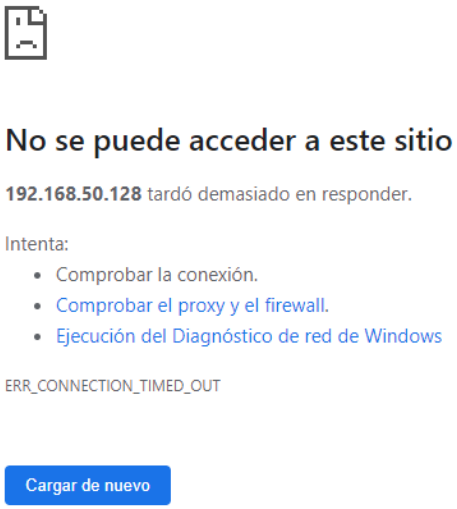


Nota. En la presente ilustración se observa los puertos abiertos por dónde se ingresa el tráfico malicio a la red interna de SITEC.

Se comprueba el ingreso al core por web, obteniendo el resultado de la denegación del ingreso hacia el router core por medio web.

Figura 18

Denegación del router core



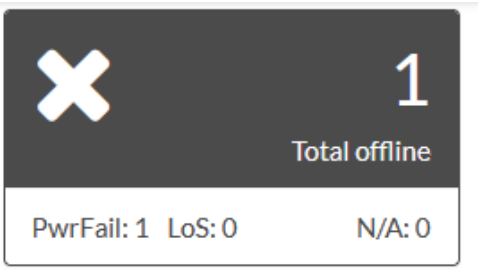
Nota. En la presente ilustración se observa la denegación del router a través del ingreso web del core de SITEC.

3.7.4.2.Ataques Físicos.

Se realiza un corte de cable de fibra óptica, obteniendo la siguiente alerta en el sistema de gestión de la red. Con esto se procede a la elaboración de la orden de trabajo y tomar la respectiva medida correctiva.

Figura 19

Corte del cable de Fibra Óptica del abonado

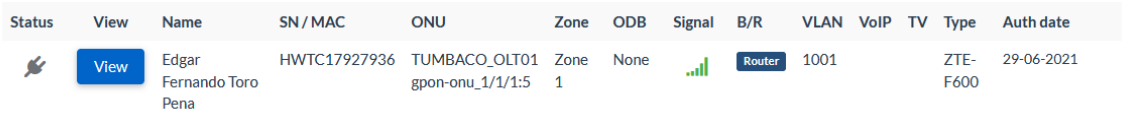


Nota. En la presente ilustración se observa el corte del cable de fibra óptica de un abonado.

Este sistema permite determinar la información del cliente, para que se facilite la reparación. Los datos necesarios de configuración y datos personales que son necesarios para el personal técnico que va a solventar el inconveniente.

Figura 20

Desconexión del abonado



Nota. En la presente ilustración se observa una desconexión de la onu de un abonado.

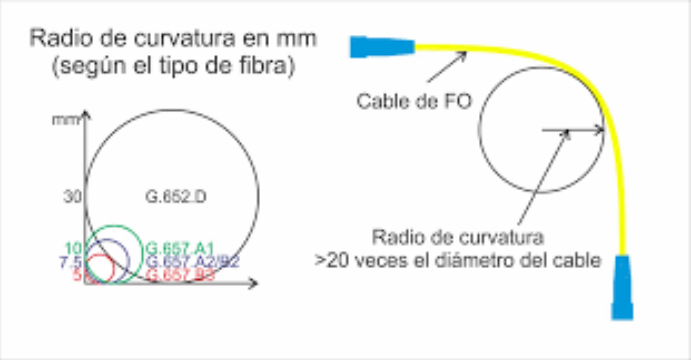
Otro problema es la curvatura del cable de fibra óptica, ya que por esto cambia las características físicas, la estructura de este cable esta formada por el Core y Cladding, por lo cual al realizar la curva del Cable la Luz (que viaja por el Núcleo) choca en mayor medida con el Cladding, produciendo una refracción de la señal que se traduce en un aumento de perdidas de potencia, es decir, mayor Atenuación.

Para determinar el radio de curvatura (Rc) máximo se debe verificar en el Datasheet del producto, el valor de Rc de cada Cable se considera antes de instalarlo.

En un caso de encontrarse en el campo de instalación y no contar con los datos del fabricante del Cable, se puede calcular con la medida del diámetro externo del Cable y multiplicado 20 veces, para obtener un valor aproximando de referencia del Radio de Curvatura. Es decir, Rc = 20 x Dc (donde Dc es el Diámetro externo de la Chaqueta del cable).

Figura 21

Radio de curvatura de la Fibra Óptica

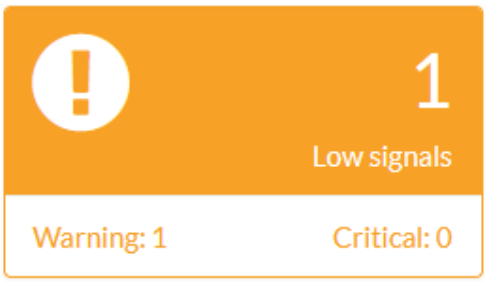


Nota. En la presente ilustración se observa el radio de curvatura permitido en tendidos de la fibra óptica.

Con la atenuaión del cable de fibra óptica, se identificaa una alerta de la misma manera, con un reporte por este evento. Cabe señalar que la potencia normal de un cliente en esta red GPON es de 15 dbm, para lo cual existe un umbral de hasta los 30 dbm, pasando este rango ya existe este tipo de alertas.

Figura 22

Alerta por atenuación del cable de Fibra Óptica



Nota. En la presente ilustración se observa una alarma en cuanto a un cliente que se encuentra con potencia alta de recepción.

Se tiene la posibilidad de desplegar la información de dicho cliente, para lo cual se procede a las correciones necesarias. Con estos datos se genera una orden de instalación para el personal técnio y se proceda con la reparación, para esto es importante conocer algunos datos que se puede visualizar en la Figura 19.

Figura 23

Información del abonado que se alerta con atenuación

Status	Signal	Signal value	Name	SN / MAC	Zone	ODB	OLT	ONU	Board	Port
		-30.87 dBm	ULQUIANGO GUANA ANA ISABEL	HWTC1792A036	Zone 1	None	TUMBACO_OLT01	TUMBACO_OLT01 gpon-onu_1/2/4:2	2	4

Nota. En la presente ilustración se observa la información del abonado que tiene el problema de potencia alta en su ONU.

El problema de este sistema es que no envía alertas de estos reportes, depende del monitoreo constante del encargado de la gestión de la red. Se debe mejorar con la implementación de un sistema que notifique los problemas de la red, ya que este modelo de negocio, se debe tener una constante disponibilidad en el servicio.

3.7.5. Análisis de Resultados.

En el ataque de DoS se tiene el siguiente análisis de tráfico, ingresado por SSH vía comandos verificamos lo Log para comprobar el ataque realizado al equipo principal de la empresa SITEC SA.

Figura 24

Ejecución del ataque DDoS

Nota. En la presente ilustración se observa la ejecución del ataque DDoS hacia la red interna de SITEC.

De la misma manera se tiene la detección de intrusos del sistema IDS en la red SDN, en la Figura 22 se tiene tres diferentes intentos de intrusión en las redes GPON.

Figura 25

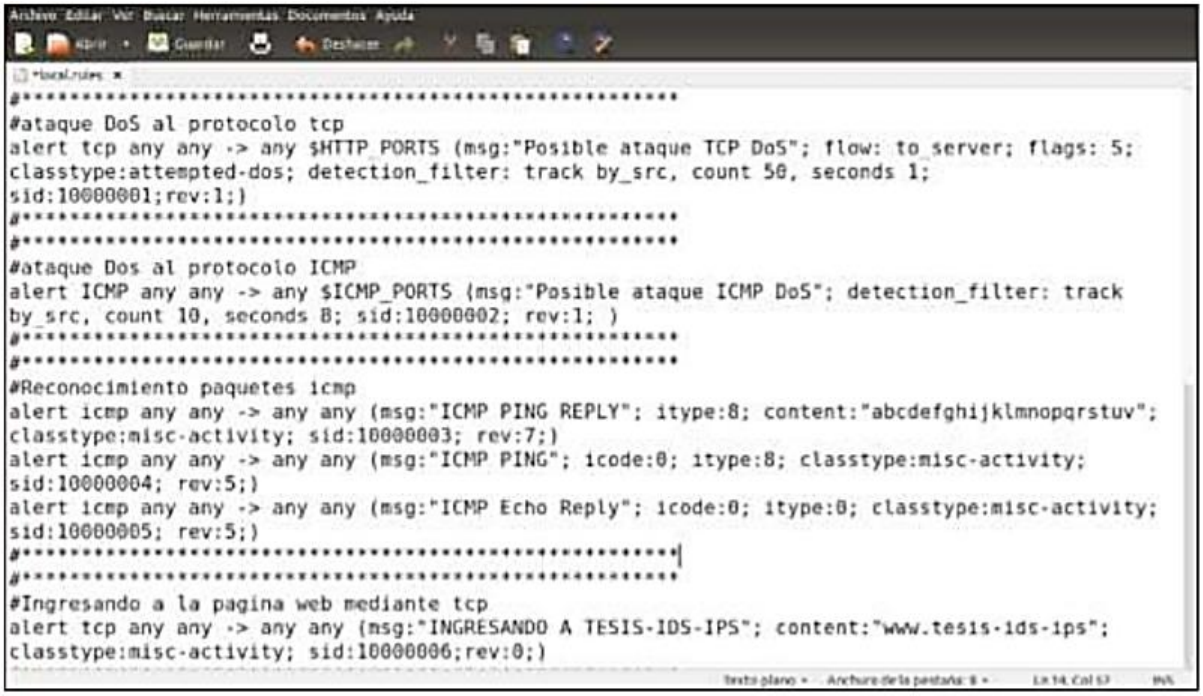
Detección de Intrusos

Nota. En la presente ilustración se observa la detección del IDS, con respecto al ataque DDoS hacia la red interna de SITEC.

La segunda prueba de estos ataques realizados es bajo la integración de un IDS en el escenario, con la ayuda del SNORT, se realizó un escaneo completo a tiempo real, conforme a las reglas establecidas, esta información invaluable es enviada al controlador para que un administrador de red tenga noción acerca de lo que está transitando por la infraestructura.

Figura 26

Reglas para detectar los intrusos



Nota. En la presente ilustración se observa las reglas que utiliza la detección del IDS, con respecto al ataque DDoS hacia la red interna de SITEC.

Medidas de Seguridad

Se citan las siguientes medidas de manera general:

- Autenticación Fuerte: no enviar contraseñas en texto plano para evitar los ataques Hombre en la mitad (MITM, Man in the Middle)
- Autenticación mutua: para evitar falsas OLT`s, estas deben ser autenticadas por las ONTs.

- Autenticación de mensajes: para evitar inyección de paquetes activos durante los ataques MITM, los mensajes más sensibles deben ser autenticados. Antivirus, anty-spy, cortafuegos, IPS/IDS y un firewall eficaz.
- Espionaje DHCP: Asegura la integridad del IP. Mantener los sistemas actualizados y parcheados. Tener a la OLT en capa 3 para configurar las ACLs y establecer filtros MAC en cada ONU.

3.8.Niveles de Riesgo según la norma ISO 27005.

Una vez que se han puesto a prueba los sistemas implementados en la red GPON de un ISP, se determina los niveles de riesgo según la norma ISO 27005. De acuerdo con el análisis de riesgos propuesta, se tiene las siguientes medidas de defensa que se han calificado de la siguiente forma.

- Cumple las mejores prácticas recomendadas.
- Necesita mejorar.
- Carencias severas.

Una vez identifica los parámetros, se procede a una entrevista a los encargados de la red de SITEC SA y a cada uno de los accionistas de esta, ya que se pretende evaluar el nivel de riesgo en cuanto al tráfico de la red GPON.

3.8.1. Ejecución de la entrevista.

La finalidad de la entrevista es recolectar información de la seguridad en la infraestructura GPON de la empresa SITEC SA, se tiene un cuestionario con preguntas abiertas

que sirven como base para tomar las medidas correctivas que mejoren la operatividad de los sistemas, brindando calidad en los servicios de internet de los abonados.

A continuación, un breve análisis de las preguntas de la entrevista:

¿El tráfico Download es propenso a que sea alterado, y a su vez afecte al funcionamiento de la red GPON?

Los proveedores de Internet requieren enviar tráfico hacia los abonados, dónde cada cliente navega acorde a la velocidad contratada, es importante el monitoreo del consumo de cada dispositivo final. La velocidad de descarga se refiere a la cantidad de megabits de datos por segundo que se necesitan para descargar datos de un servidor en forma de imágenes, videos, texto, archivos y audio.

¿El tráfico Upload es propenso a que sea alterado, y a su vez afecte al funcionamiento de la red GPON?

La velocidad de carga se refiere a la cantidad de megabits de datos por segundo que puede enviar información desde su computadora a otro dispositivo o servidor en Internet. La transferencia de información es lo que hace susceptible a colapsos de información si no se encuentra debidamente monitoreado.

¿Qué tan probable son los cortes del cable de fibra óptica?

En una red GPON se tiene dos escenarios, el primero es una infraestructura soterrada la que permite un cierto grado de protección al cable de fibra óptica, y el segundo escenario es de tener la infraestructura aérea, es decir que el tendido del cable se lo hace a través de los postes instalados lo que hace que sea más riesgoso y propenso a cortes con respecto al primero.

¿Se considera un problema grave las atenuaciones por micro curvatura en el cable de fibra óptica?

La fibra óptica tiene como debilidad la micro curvatura, esto es debido a la fabricación de este cable, ya que tiene como material vidrio el mismo que hace que este medio guiado sufra de este problema, para esto se debe implementar buenas prácticas en la construcción de redes GPON.

¿La empresa cuenta con algún sistema que detecte tráfico malicioso?

Existen sistemas que analizan el tráfico, y tener un constante monitoreo; adicional a esto se es primordial contar con un sistema que detecte tráfico malicioso, con la finalidad de solventar problemas de velocidad de los abonados.

¿Cómo evalúan el tráfico inusual?

Existen en el mercado soluciones tecnológicas que permiten la detección de tráfico inusual, es importante contar con estos sistemas que evalúen la transferencia de datos y pueda garantizar la integridad de la información que viaja de un punto a otro.

¿El personal está capacitado para solventar problemas de seguridad?

En las empresas de telecomunicaciones es indispensable que el personal a cargo de las TI cuenten con los conocimientos de seguridad de redes, ya que toda infraestructura de datos es susceptible a vulneraciones.

3.8.2. Resultados del análisis de riesgos.

En la Tablas 5 se muestra la evaluación actual de la red GPON en base al criterio técnico que se evaluó en el transcurso de la investigación mediante el análisis de tráfico y la

implementación de la metodología Offensive Security. Adicional, se realizó un método investigativo de entrevista que nos permitió recolectar información importante del ISP para apoyar al resultado de los niveles de riesgo.

Se recomienda siempre estar a la vanguardia en el estudio de la seguridad, ya que, así como se va mejorando la seguridad, los delincuentes informáticos buscan nuevas formas de vulnerar la red de su objetivo. A continuación, un detalle por área:

En el área de Infraestructura, se tiene un nivel crítico ya que tenemos los equipos de la red GPON y los equipos del nodo. Aquí, tenemos la importancia de proteger los datos y la disponibilidad de los equipos.

En el área de Servicios se tiene las aplicaciones que dan soporte para la activación y monitoreo de la red, la misma que es crítico ya que la información es delicada en esta área.

Para las Operaciones tenemos un nivel medio, ya que se tiene normativas establecidas para el despliegue de redes GPON. De la misma manera la parte de personal se tiene capacitado en cada una de las funciones y en base a las seguridades correspondientes, por ello se tiene un nivel medio.

Tabla 5

Análisis de Riesgos

ÁREAS EVALUADAS	ANÁLISIS DE RIESGOS
Infraestructura	
Servicios	

Operaciones	
Personal	

Nota. En la siguiente tabla se muestra el análisis de tráfico del software Microsoft Security Assessment Tool.

CAPITULO IV

DISEÑO E IMPLEMENTACIÓN

Este capítulo enmarca una solución mediante el diseño de un IDS en redes SDN que mejore el sistema de identificación de tráfico malicioso, para este caso se va a realizar pruebas en un entorno real, en una infraestructura GPON de la empresa SITEC. Se tiene una solución que se va a analizar el costo-beneficio, el cual permitirá validar que es una solución rentable para este modelo de negocio.

4.1.Diseño de un IDS en una SDN en la Infraestructura GPON.

Una vez terminado la ejecución de la Metodología Offensive Security e identificado los niveles de riesgo, se tiene como propuesta realizar un diseño de un IDS en una SDN para brindar una mejora en cuanto a la seguridad de la red GPON. Para esto se requiere la implementación de un entorno de simulación en dónde se realiza las verificaciones necesarias para posteriormente ser implementado y probado en un ambiente real.

4.1.1. Requerimientos para el diseño del IDS.

En esta sección es necesario analizar los requerimientos de software y hardware para la implementación del diseño de un IDS en redes SDN, con esta solución se pretende mejorar el sistema de seguridad por medio de un detector de intrusos que notifique al administrador de la red los fallos que se

Software

-La distribución de CentOS Linux es una plataforma estable, predecible, administrable y reproducible derivada de las fuentes de Red Hat Enterprise Linux (RHEL). Se pretende usar la versión 7 de Centos ya que es un sistema operativo que se puede instalar Mininet para la

implementación de SDN, de igual manera se puede montar un IDS con SNORT, lo que lo hace el sistema operativo ideal para la implementación en la red GPON.

- SNORT IDS usa una serie de reglas que ayudan a definir la actividad de red maliciosa y usa esas reglas para encontrar paquetes que coincidan con ellas y genera alertas para los usuarios. Adicional, a este uso se implementará el IDS en una red SDN, para esto se requiere la instalación del controlador SDN Virtual Application Networks (VAN) de HP, ya que este permite un control centralizado e integra los sistemas.

- Mininet es un emulador de red que ejecuta una colección de máquinas, conmutadores, enrutadores y enlaces en un único kernel de Linux. Se pueden utilizar conexiones SSH en él, y ejecutar programas arbitrarios. Los programas que se ejecutan pueden mandar paquetes, con una velocidad de enlace y retraso asignado previamente. Los paquetes son procesados como si de una red real se tratase, con sus consiguientes colas a la hora de procesar los paquetes. Red Mininet formada por dos máquinas. Se pueden crear topologías lineales, simples, en forma de árbol, o bien se pueden programar de una forma específica según las necesidades.

Hardware

- ONT de prueba para simular los ataques que permitan validar la implementación del IDS en una red SDN.
- Computador donde se encuentra instalado Kali Linux con la finalidad de hacer los ataques de intrusión y validar el diseño.

El autor (Morales Dávila, 2018) realiza un diseño de un IDS en un entorno SDN, para esto requirió de un ordenador con las características que se observa en la Tabla 6

Tabla 6

Comparación de Hardware diseño e implementación

Requerimientos Diseño		**Requerimientos**	**Producción**
Parámetros	Valores	Parámetros	Valores
Procesador	Intel Core 2 Duo de 2.93Ghz	Procesador	2.1 GHz Intel Xeon D-1541 Eight-Core
RAM	2 Gb	RAM	16 Gb
Fuente de Alimentación	Uno de 250W	Fuente de Alimentación	Redundante de 800W
Almacenamiento	500Gb	Almacenamiento	1 Tb

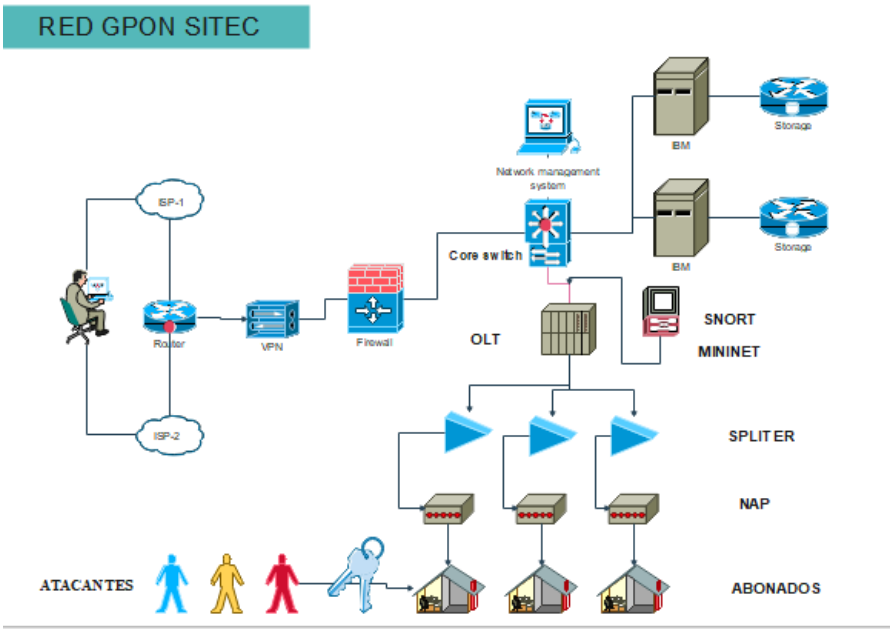
Nota. En la siguiente tabla se muestra el análisis comparativo entre un servidor para diseño y uno que soporte el tráfico de un Proveedor de Servicios.

4.1.2. Topología

Una vez realizado el análisis de tráfico, la implementación de la Metodología Offensive Security y determina los niveles de riesgo, se hace la propuesta de la siguiente topología, la cual permitirá mejorar el sistema de gestión de seguridad de la red GPON.

Figura 27

Topología del diseño de un IDS en redes SDN



Nota. En la presente ilustración se observa la topología del diseño de un IDS en redes SDN de la red interna de SITEC.

4.2.Ataques Informáticos para SDN/OpenFlow

La seguridad en una SDN es de suma importancia ya que se está migrando las redes tradicionales a esta nueva tecnología, sin embargo, los ataques son cada vez más complejos y son diseñados con el objetivo de vulnerar una red SDN. Por lo tanto, se analiza los posibles ataques a los elementos de red, como puede ser el controlador, el switch open Flow o los hosts,

4.2.1. Escanning

Este ataque consiste en obtener información relevante sobre el objetivo, en una red SDN se podría obtener la topología, las características de los hosts o los detalles de la comunicación entre los switches y el controlador.

4.2.2. Spoofing

Es un ataque que consiste en hacerse pasar por uno de los elementos de la red, puede ser un switch, un host o el controlador. Si el controlador es manipulado se podría generar flujos de entrada ocasionando el control total de la red.

4.2.3. DDoS

Un ataque Dos o DDoS consiste en inhabilitar los recursos de una red, en una red SDN se puede enviar varios flujos legítimos hacia un switch openflow, hasta el punto de que la Flow Table ya no pueda almacenar flujos de los elementos de red. Si el ataque se realiza al controlador, se podría dar el caso de un ataque de TCAM exhaustion, donde se podría usar una Bonet en la cual se envían varias solicitudes por el segundo controlador consiguiendo de esta forma saturar la TCAM y alterar el funcionamiento de la red.

Inundación UDP (Protocolo de Datagramas de Usuario). - Este ataque envía paquetes falsos de conexión, incapacitando la asociación con las aplicaciones, dando mensajes de error hasta sobrecargar el sistema y denegarlo.

Inundación SYN. - Este ataque consiste en paralizar el proceso de SYN, mediante el envío de múltiples solicitudes, el sistema colapsa ya que espera el ACK de cada solicitud de conexión, atascando los recursos hasta que no se pueda realizar nuevas conexiones y como resultado se obtiene la denegación de servicio.

Inundación ICMP. - Es un ataque que consiste en la utilización masiva del protocolo ICMP el cual consiste en diagnosticar errores a través del comando ping y probar conectividad de los sistemas. Este ataque es simplemente una avalancha de solicitudes de ping obstruyendo peticiones reales.

4.3.Funcionamiento de la SDN con IDS.

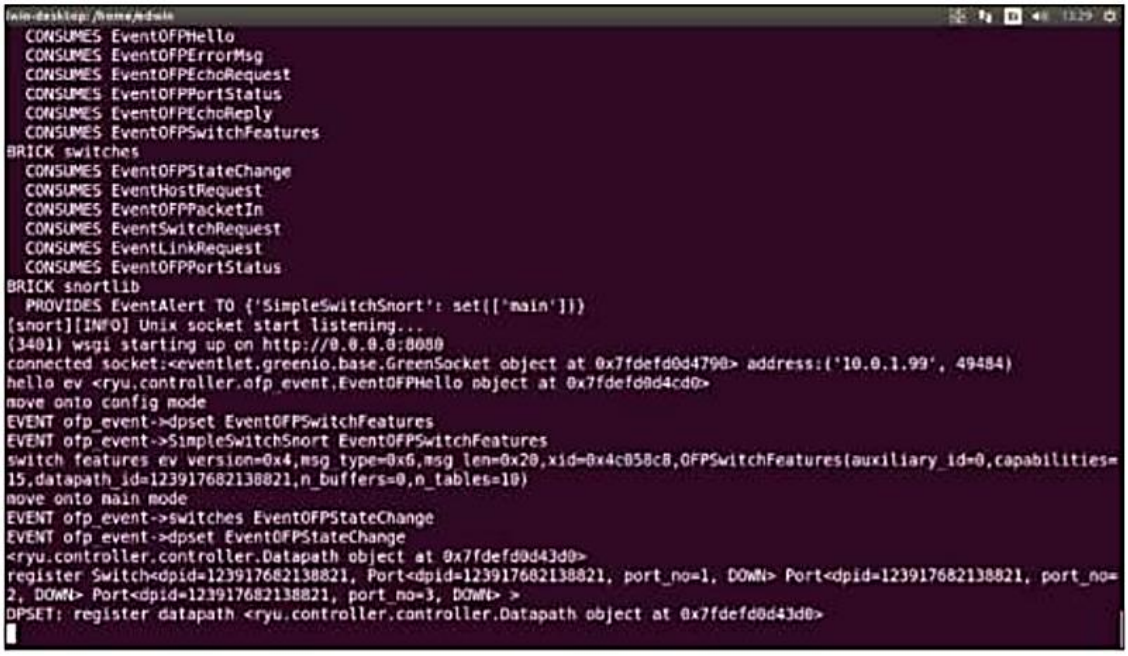
Luego de instalar el Snort, se agrega un conjunto de reglas para detectar los ataques a la red, si se añaden muchas reglas no significa que detectará más actividades sospechosas, lo contrario muchas reglas genera una sobrecarga en el procesamiento teniendo así una tasa de perdidas muy elevada de paquetes no analizados.

La plataforma Ryu solo está disponible para sistemas operativos Linux, por ello se opta usar Ubuntu 14.04 LTS, el cual está basado en la arquitectura Debían, Ubuntu en un S.O de acceso libre para computadoras, lo puede utilizar un usuario sin tener grandes conocimientos gracias a la simplicidad y de fácil interactividad, además existe mucha documentación gratuita para comprender el funcionamiento de todas herramientas disponibles.

El siguiente paso, es ejecutar esta aplicación con el controlador Ryu mediante la terminal del Ubuntu. Pero para lograr este cometido, se debe usar la herramienta ryu-manager, la cual debe ejecutarse exitosamente tal como se muestra en la Figura 24, y en caso de inconvenientes, verificar la correcta instalación del Ryu.

Figura 28

Controlador Ryu



Nota. En la presente ilustración se observa las configuraciones del controlador RYU para la SDN de la red interna de SITEC.

4.3.1. Pruebas de conectividad.

Una vez habilitados los servicios, se procedió a realizar pruebas para comprobar la conectividad y funcionalidad, mediante el envío de paquetes IP, para que posteriormente estos sean detectados por el sistema SNORT, y luego enviar la información obtenida al controlador RYU.

En esta sección se determinó el perfomance o rendimiento de una red SDN versus una red tradicional, para esto se realizó pruebas con la finalidad de obtener los tiempos de respuesta cuando la red se encuentra sin o con un flujo abundante de tráfico.

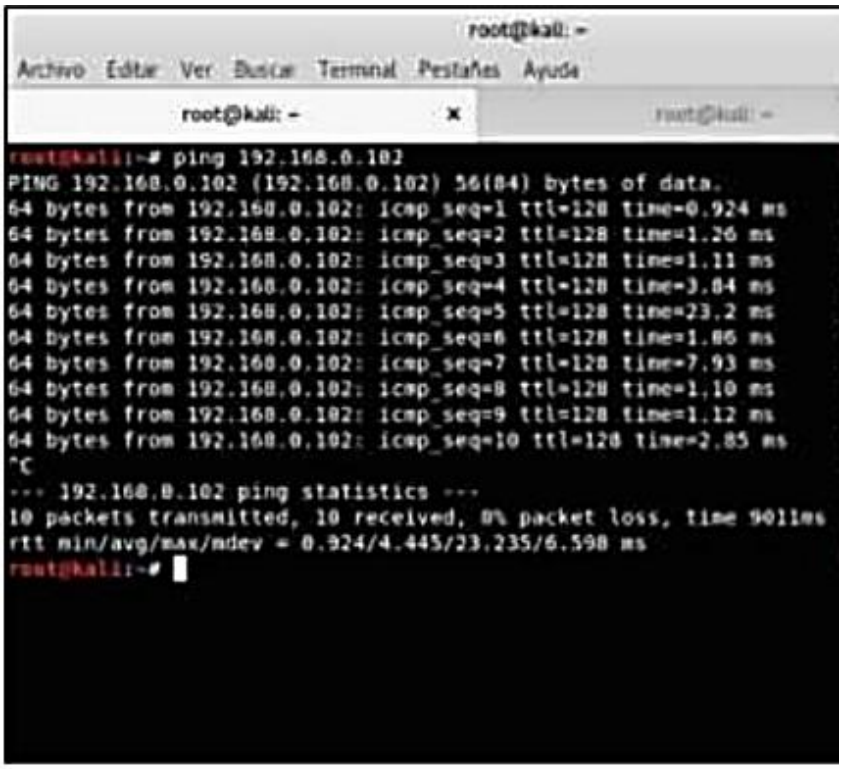
A continuación, los escenarios:

- Escenario 1: Se tiene una red GPON con un IDS.
- Escenario 2: Se tiene una red GPON con un IDS con un atacante.
- Escenario 3: Se tiene una red GPON con un IDS en una red SDN.
- Escenario 4: Se tiene una red GPON con un IDS en una red SDN con atacante.

Para ello se generaron 10 paquetes ICMP, tanto en el primer como en el segundo escenario. En la Figura 29, muestra los tiempos de respuesta cuando la red se encuentra sin tráfico de datos, obteniendo como promedio 1.7835 milisegundos, en la Figura 30 muestra los tiempos de respuesta cuando la red se encuentra bajo ataques DoS, teniendo como promedio 12.2697 milisegundos.

Figura 29

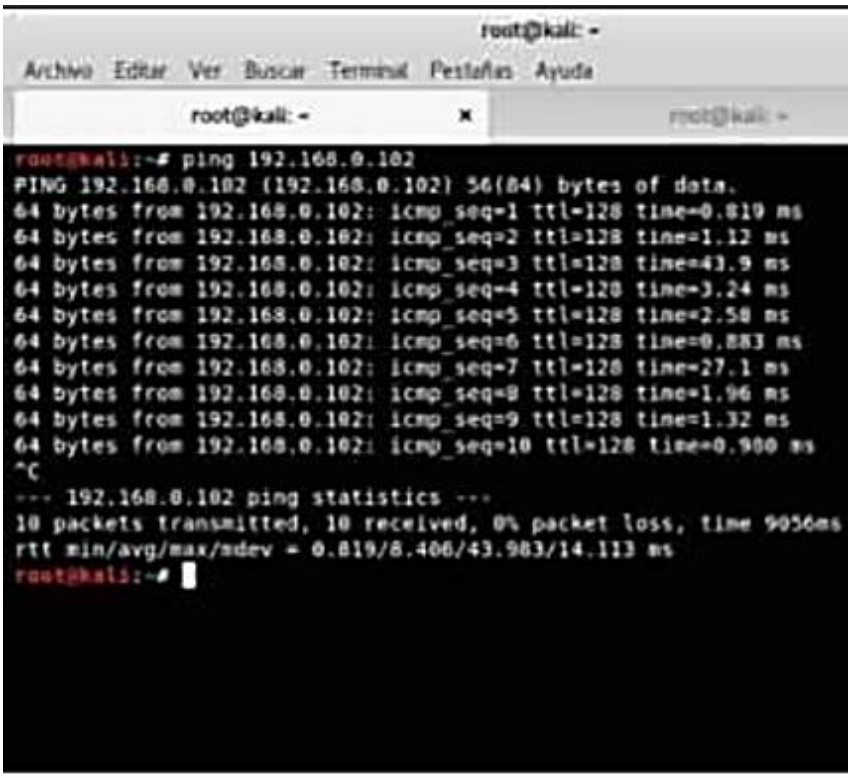
Tiempos de respuesta IDS sin SDN sin ataque



Nota. En la presente ilustración se observa los tiempos de respuesta de la conexión del IDS antes de tener una red SDN y sin atacante.

Figura 30

Tiempos de respuesta IDS sin SDN con ataque

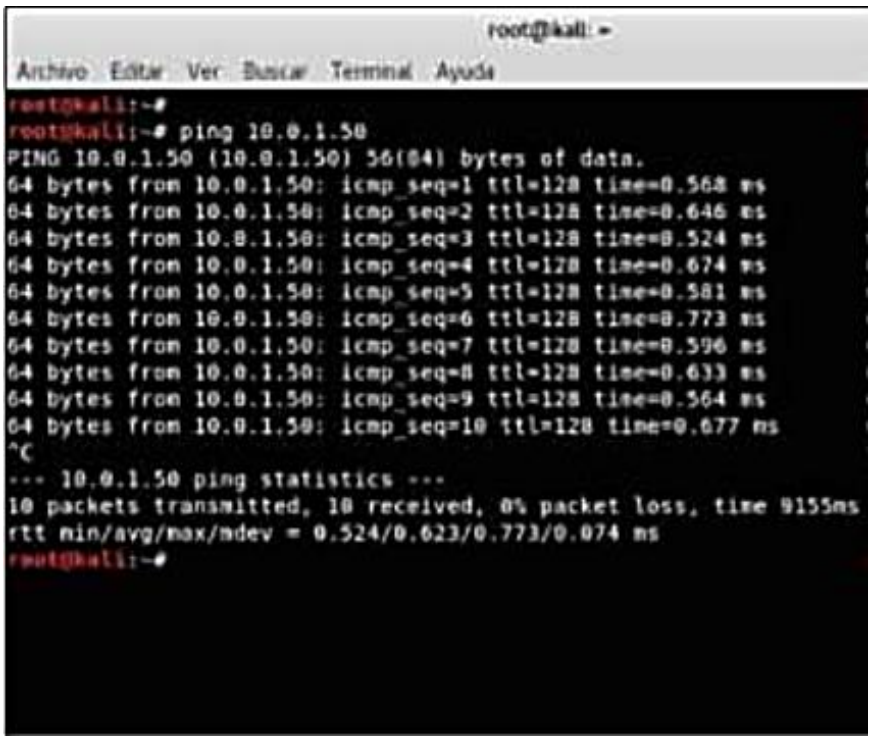


Nota. En la presente ilustración se observa los tiempos de respuesta de la conexión del IDS antes de tener una red SDN con atacante.

Se realizó las pruebas anteriores, teniendo como respuesta la Figura 31 la evidencia un promedio de tiempo de respuesta de 0.603 milisegundos, mientras que en la Figura 32 un valor de 1.3887 milisegundos como media del tiempo de respuesta cuando la red se encuentra bajo ataques.

Figura 31

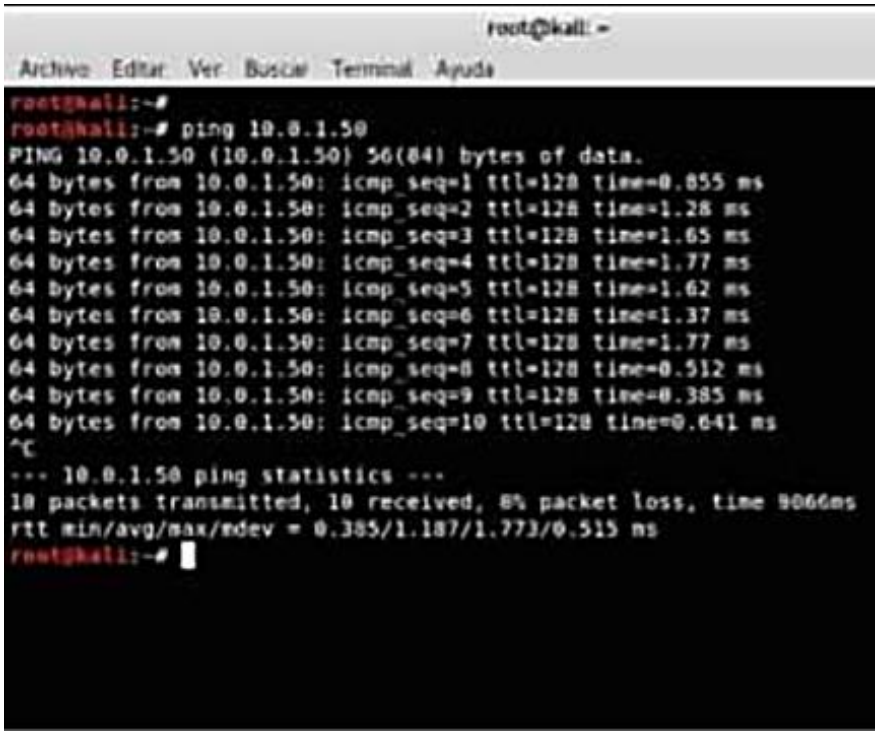
Tiempos de respuesta IDS con SDN sin ataque



Nota. En la presente ilustración se observa los tiempos de respuesta de la conexión del IDS implementado la red SDN sin atacante.

Figura 32

Tiempos de respuesta IDS con SDN con ataque



Nota. En la presente ilustración se observa los tiempos de respuesta de la conexión del IDS implementado la red SDN con atacante.

En la Tabla 7 se realiza una comparación de los tiempos de respuesta en los distintos escenarios de pruebas, en primer caso es un IDS sin SDN sin Ataque el mismo que presenta tiempos normales, el segundo caso es un IDS sin SDN con Ataque lo que notoriamente se tiene un incremento notorio en cuanto a los tiempos de respuesta. Una vez implementado la solución del diseño, el cual consiste en implementar una red IDS con SDN en la red GPON de SITEC, se tiene el tercer caso que es un IDS con SDN sin ataque el cual mejora los tiempos, y por último caso es un IDS con SDN con ataque el cual mitiga considerablemente el ataque reduciendo los tiempos en comparación a la red tradicional, dando como resultado positivo la implementación de un IDS en redes SDN para mejorar la disponibilidad de los Proveedores de Internet.

Tabla 7

Comparación de tiempos de respuesta en la red

TIEMPOS	*IDS SIN SDN SIN ATAQUE*	*IDS SIN SDN CON ATAQUE*	*IDS CON SDN SIN ATAQUE*	*IDS CON SDN CON ATAQUE*
TIEMPO 1	*0.924*	*0.819*	*0.568*	*0.855*
TIEMPO 2	*1.26*	*1.12*	*0.646*	*1.28*
TIEMPO 3	*1.11*	*43.9*	*0.524*	*1.65*
TIEMPO 4	*3.84*	*3.24*	*0.674*	*1.77*
PROMEDIO	*1.7835*	*12.2697*	*0.603*	*1.3887*

Nota. En la siguiente tabla se muestra el análisis de tiempos de respuesta en la red de SITEC antes del diseño y después de la implementación de la red SDN con IDS.

4.3.2. Pruebas de funcionamiento con Ataques DDoS.

En este apartado se ejecutará ataques de DDoS para validar el funcionamiento de las infraestructuras de red, para lo cual se requiere evaluar el IDS sin SDN o red tradicional previo a la implementación del diseño de un IDS en SDN, para finalmente hacer una comparación entre las dos topologías.

A Continuación, los parámetros para la evaluación de los sistemas:

Tiempo 1.- 5 minutos

Tiempos 2.- 10 minutos

Tiempo 3.- 15 minutos

Paquetes. - Es la cantidad de paquetes procesados por el Snort.

Pkts/min. - Es la cantidad de paquetes detectados por minuto.

Cpu. - Carga que tiene el CPU en los tiempos.

Tiempo de detección de alerta. - Es el tiempo que se demora Snort en

El primer ataque para ejecutarse es el de inundación por UDP, el cual consiste en atacar al protocolo sin conexión, a continuación, se tiene el comando:

Hping3 –rand-source –udp 192.168.50.128 -p 80 –faster

-rand-source: Ip de origen aleatorio.

-udp: protocolo de datagramas de usuario.

-p: es el Puerto al cuál se pretende llegar las peticiones.

-faster: envío rápido de peticiones.

En el primer escenario para este ataque de inundación UDP se tiene los siguientes resultados:

Tabla 8

Inundación UDP sin SDN

	Tiempo 1	**Tiempo 2**	**Tiempo 3**	**PROMEDIO**
Paquetes	168	342	716	408
Pkts/min	33	34	47	38
Alertas	164	336	712	404
CPU	15%	20%	38%	24%
Tiempo de detección de alertas	0.55s	0.56s	0.78s	0.63s

Nota. En la siguiente tabla se muestra el análisis de tiempos de respuesta del ataque de Inundación UDP en un IDS sin SDN.

En el segundo escenario para este ataque de inundación UDP se tiene los siguientes resultados:

Tabla 9

Inundación UDP en una red SDN

	Tiempo 1	**Tiempo 2**	**Tiempo 3**	**PROMEDIO**
Paquetes	170	348	722	413
Pkts/min	34	36	49	40
Alertas	169	345	718	411
CPU	10%	12%	19%	14%
Tiempo de detección de alertas	0.52s	0.54s	0.74s	0.60s

Nota. En la siguiente tabla se muestra el análisis de tiempos de respuesta del ataque de Inundación UDP en un IDS en una red SDN.

El segundo ataque para ejecutarse es el de inundación por SYN, para este caso se hace una modificación en cuanto a la cantidad de paquetes enviados, para este caso 500 bytes de información adicional, a continuación, se tiene el comando:

Hping3 –rand-source –syn -d 500 192.168.50.128 -p 80 –faster

-rand-source: Ip de origen aleatorio.

-syn: protocolo de sincronización.

-p: es el Puerto al cuál se pretende llegar las peticiones.

-faster: envío rápido de peticiones.

En el primer escenario para este ataque de inundación SYN se tiene los siguientes resultados:

Tabla 10

Inundación SYN en una red sin SDN

	Tiempo 1	**Tiempo 2**	**Tiempo 3**	**PROMEDIO**
Paquetes	84168	171987	358334	204830
Pkts/min	16834	17199	23889	19307
Alertas	83326	170267	354751	202781
CPU	22%	35%	52%	36%
Tiempo de detección de alertas	0.57s	0.62s	0.79s	0.66s

Nota. En la siguiente tabla se muestra el análisis de tiempos de respuesta del ataque de Inundación SYN en un IDS en una red sin SDN.

En el segundo escenario para este ataque de inundación UDP se tiene los siguientes resultados:

Tabla 11

Inundación SYN en una red SDN

	Tiempo 1	**Tiempo 2**	**Tiempo 3**	**PROMEDIO**
Paquetes	85017	174348	361722	207029
Pkts/min	17003	17434	24115	17517

Alertas	84167	172604	358105	204959
CPU	14%	19%	24%	19%
Tiempo de detección de alertas	0.53s	0.58s	0.71s	0.61s

Nota. En la siguiente tabla se muestra el análisis de tiempos de respuesta del ataque de Inundación SYN en un IDS en una red SDN.

El tercer ataque para ejecutarse es el de inundación por ICMP, este comando consiste en inundar de peticiones de conectividad al destino, para este caso se modifica el tamaño de los paquetes a 1000 bytes, a continuación, se tiene el comando:

Hping3 –rand-source –icmp -d 1000 192.168.50.128 -p 80 –faster

-rand-source: Ip de origen aleatorio.

-icmp: solicitud de conexión ping.

-p: es el Puerto al cuál se pretende llegar las peticiones.

-faster: envío rápido de peticiones.

En el primer escenario para este ataque de inundación ICMP se tiene los siguientes resultados:

Tabla 12

Inundación ICMP en una red sin SDN

	Tiempo 1	**Tiempo 2**	**Tiempo 3**	**PROMEDIO**
Paquetes	168123	342234	716546	408968

Pkts/min	33625	34223	47770	38539
Alertas	166442	338812	709381	404878
CPU	25%	42%	64%	44%
Tiempo de detección de alertas	0.54s	0.61s	0.73s	0.62s

Nota. En la siguiente tabla se muestra el análisis de tiempos de respuesta del ataque de Inundación ICMP en un IDS en una red sin SDN.

En el segundo escenario para este ataque de inundación UDP se tiene los siguientes resultados:

Tabla 13

Inundación ICMP en una red SDN

	Tiempo 1	**Tiempo 2**	**Tiempo 3**	**PROMEDIO**
Paquetes	170644	348567	722978	414063
Pkts/min	853220	34857	48199	312092
Alertas	168938	345081	715748	409922
CPU	19%	24%	29%	24%
Tiempo de detección de alertas	0.53s	0.55s	0.69s	0.59s

Nota. En la siguiente tabla se muestra el análisis de tiempos de respuesta del ataque de Inundación ICMP en un IDS en una red SDN.

Por último, se tiene un análisis final de los resultados obtenidos en lo tres ataques de DDoS, se tiene una leve variación en cuánto a los tiempos de respuesta de las alertas con respecto a las redes sin SDN y con SDN, pero lo más notorio es el nivel de CPU que se tiene en los escenarios ya que esta nueva tecnología permite optimizar recursos de procesamiento al momento de identificar tráfico malicioso.

Tabla 14

Comparación de resultados de ataques DDoS

	RED IDS SIN SDN			**RED IDS CON SDN**		
	Inundación UDP	**Inundación SYN**	**Inundación ICMP**	**Inundación UDP**	**Inundación SYN**	**Inundación ICMP**
Paquetes	408	204830	408968	413	207029	414063
Pkts/min	38	19307	38539	40	17517	312092
Alertas	404	202781	404878	411	204959	409922
CPU	24%	36%	44%	14%	19%	24%
Tiempo de detección de alertas	0.63s	0.66s	0.62s	0.60s	0.61s	0.59s

Nota. En la siguiente tabla se muestra el análisis comparativo del funcionamiento de un IDS implementado en una red tradicional y una red SDN.

4.4.Análisis de costo

El análisis de costo corresponde a todo lo que se utilizó para la implementación del diseño del IDS en las redes SDN y la evaluación previa para llegar a obtener la información necesaria para ser implementadas, incluyendo el uso de los equipos que se encuentran en la red GPON de la empresa SITEC.

Se realizó configuraciones en los equipos de pruebas que se encuentran en la red GPON, para posteriormente ser revisadas y aprobadas por parte del personal de SITEC SA para que sean implementadas en el ambiente de producción. Los servidores que se manipuló usan software libre y privado, dónde se analiza el costo de las licencias de ser el caso, en mencionado análisis de costo se toma en cuenta el software y hardware necesario para la elaboración del proyecto.

4.4.1. Presupuesto.

Para el diseño se requiere de dos ordenadores para la realización del pen testing, uno colocado en la red del abonado con la herramienta Kali Linux para la inyección de tráfico malicioso y otro en el lado de la infraestructura de red Interna que contiene el IDS en la red SDN. Se deja como propuesta la adquisición de un servidor para la instalación de un IDS en una red SDN.

Tabla 15

Presupuesto Hardware Diseño

Hardware	**Cantidad**	**Precio U.**	**Valor (USD)**
Laptop Dell i7	2	$ 0.00	$ 0.00
Total			$ 0.00

Nota. En la siguiente tabla se muestra el costo en cero del hardware del diseño ya que se utiliza herramientas personales para simulación.

Para el pen testing e implementación de soluciones, todas las herramientas utilizadas corresponden a Open Source, con esto se tiene la finalidad de mejorar la seguridad de la red GPON de SITEC SA se recomienda su adquisición de los siguientes sistemas, el detalle económico se detalla en la Tabla 9.

Tabla 16

Hardware de la Implementación del diseño

Hardware	**Cantidad**	**Precio U.**	**Valor (USD)**
Servidor IDS/IPS	1	$ 5399.99	$ 5399.99
Total			$ 5399.99

Nota. En la siguiente tabla se muestra el costo de un servidor con las características necesarias para la implementación en un ambiente real.

En la Tabla 10 se tiene los costos del software, en este caso será el mismo valor ya que se necesita de los mismos programas y sistemas para poder implementar la solución de seguridad informática.

Tabla 17

Presupuesto Software Adicional

Software	**Cantidad**	**Precio U.**	**Valor (USD)**
Mininet	1	$ 0.00	$ 0.00

MSAT 3.0	1	$ 0.00	$ 0.00
Kali Linux	1	$ 0.00	$ 0.00
FOCA	1	$ 0.00	$ 0.00
WinSCP	1	$ 0.00	$ 0.00
PUTTY	1	$ 0.00	$ 0.00
ZOC7	1	$ 0.00	$ 0.00
Linset	1	$ 0.00	$ 0.00
Wireshark	1	$ 0.00	$ 0.00
Pfsense	1	$ 0.00	$ 0.00
Total			$ 0.00

Nota. En la siguiente tabla se muestra el costo en cero del software ya que son sistemas open source.

Por último, para la propuesta de ser implementado se requiere contratar mantenimiento y actualizaciones del servidor, es recomendable realizarlo cada 3 meses; adicional, un presupuesto para eventualidades que es el 10% del costo del servidor los costos se muestran en la Tabla 10.

Tabla 18

Otros Gastos

Otros Gastos	**Cantidad**	**Precio U.**	**Valor (USD)**
Mantenimiento IDS en SDN	1	$ 400	$ 400
Presupuesto para Imprevistos	1	$ 539.99	$ 539.99
Instalación IDS-IPS en SDN	1	$ 500	$ 500
Total			$ 1439.99

Nota. En la siguiente tabla se muestra el costo del mantenimiento del servidor y un presupuesto para cualquier tipo de eventualidad.

4.4.2. Costo Beneficio.

El presente proyecto de titulación se realizó con fines educativos, orientado a la mejora en la seguridad de las redes GPON que se encuentran en producción, tuvo la finalidad de optimizar recursos existentes de la empresa SITEC SA, con finalidad de proponer una mejora en el equipamiento e implementación de medidas preventivas y correctivas, para que de esta manera el ISP siempre esté a la vanguardia en cuando seguridad informática y brinde un servicio de calidad en beneficio de los abonados.

Tabla 19

Análisis de Costos

Descripción	**Costos en Diseño (USD)**	**Costos en la implementación (USD)**
Hardware	$ 0.00	$ 5399.99
Software Adicional	$ 0.00	$ 0.00
Otros Gastos	$ 0.00	$ 1439.99
Total	$ 0.00	$ 6839.98

Nota. En la siguiente tabla se muestra una comparación entre el costo de diseño y el costo que conlleva la implementación de esta solución.

Se tiene que tomar en cuenta que la solución se recomienda ser implementada, para esto se tiene en la Tabla 13 un análisis del dinero que puede perder el ISP por ser afectado en la disponibilidad del servicio.

Tabla 20

Ingresos mensuales SITEC

Descripción	Precio de Planes	Clientes	TOTAL
Plan Básico	$ 16.99	50	$ 849.50
Plan Clásico	$ 19.99	68	$ 1359.32
Plan Máster	$ 22.99	42	$ 965.58
Plan Fourios	$ 29.99	35	$ 1049.65
TOTAL		195	$ 4224.05

Nota. En la siguiente tabla se muestra los ingresos mensuales de la empresa SITEC de una zona de cobertura.

Un ataque informático, tiene como finalidad vulnerar los servicios y perder la disponibilidad de estos; para lo cual la implementación de un IDS en redes SDN es de suma importancia para los proveedores de Internet ya que corre el riesgo de perder clientes lo cual afectara a los ingresos económicos mensuales de la empresa. No se podría calcular las pérdidas financieras exactamente ya que esto depende del tiempo de respuesta ante un ataque y el comportamiento de los abonados ante esta situación, debito a esto se realiza un método investigativo de encuesta a los dueños de SITEC SA, para sustentar con experiencia del negocio este problema de disponibilidad y su comportamiento en el mercado.

A continuación, las preguntas realizadas al personal de SITEC SA:

¿Qué grado de afectación tiene una caída total del servicio entre 1 a 30 minutos?

1. **Nivel bajo**
2. Nivel medio

3. Nivel alto

¿Qué grado de afectación tiene una caída total del servicio entre 30 minutos a 2 horas?

1. **Nivel bajo**
2. Nivel medio
3. Nivel alto

¿Qué grado de afectación tiene una caída total del servicio entre 2 a 4 horas?

1. Nivel bajo
2. **Nivel medio**
3. Nivel alto

¿Qué grado de afectación tiene una caída total del servicio ente 4 a 12 horas?

1. Nivel bajo
2. **Nivel medio**
3. Nivel alto

¿Qué grado de afectación tiene una caída total del servicio ente 12 a 24 horas?

1. Nivel bajo
2. Nivel medio
3. **Nivel alto**

¿Enumere del 1 al 4 el plan de internet según la exigencia del grupo de usuarios?

Plan Básico **1**

Plan Clásico **1**

Plan Máster **2**

Plan Fourios **4**

En la Tabla 14 se tiene el resultado de la encuesta al personal de SITEC SA, la misma que detalla la cantidad de clientes retirados por indisponibilidad de su servicio de Internet en su hogar. Se tiene varios escenarios en lapsos de tiempo de los cortes de servicio, para realizar un análisis minucioso en cuanto a problemas de disponibilidad.

Tabla 21

Pérdida de Clientes por indisponibilidad.

Descripción	**De 1 a 30 minutos**	**De 30 minutos a 2 horas**	**De 2 horas a 4 horas**	**De 4 horas a 12 horas**	**De 12 horas a 24 horas**
Plan Básico	0	0	0	1	2
Plan Clásico	0	0	1	2	2
Plan Máster	0	1	1	2	4
Plan Fourios	1	1	2	4	6
TOTAL	1	2	4	9	14

Nota. En la siguiente tabla se tiene un aproximado de pérdidas de clientes acorde al plan de Internet y al tiempo de corte total del servicio.

En la Tabla 15 se tiene un análisis similar, pero en este caso se realiza un análisis económico en base a los precios de los planes de Internet. Cabe señalar la importancia de

solucionar problemas de seguridad en el menor tiempo ya que entre más tiempo sea la respuesta más son las pérdidas económicas por un mal servicio.

Otro punto importante es brindar un servicio bajo las normas de calidad emitidas por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) en cuanto al porcentaje de disponibilidad que se debe brindar al cliente, ya que faltando a esta disposición puede acarrear multas por este ente regulador.

Tabla 22

Pérdida económica por indisponibilidad del servicio

Descripción	De 1 a 30 minutos	De 30 minutos a 2 horas	De 2 horas a 4 horas	De 4 horas a 12 horas	De 12 horas a 24 horas
Plan Básico	0	0	0	$ 16.99	$ 33.98
Plan Clásico	0	0	$ 19.99	$ 39.98	$ 39.98
Plan Máster	0	$ 22.99	$ 22.99	$ 45.98	$ 91.96
Plan Fourios	$ 29.99	$ 29.99	$ 59.98	$ 119.96	$ 179.94
TOTAL	$ 29.99	$ 52.98	$ 102.96	$ 222.91	$ 345.86

Nota. En la siguiente tabla se tiene un aproximado de pérdidas económicas acorde al plan de Internet y al tiempo de corte total del servicio.

Beneficio.

El ISP SITEC SA se benefició con una mejora en cuanto a la seguridad informática de la red interna, sobre todo en lo que respecta a la infraestructura GPON. Mediante la implementación del diseño de un IDS en redes SDN, el cual permite mejorar el sistema de seguridad.

El presente proyecto implícitamente tiene beneficio económico, ya que la finalidad de la auditoría informática es solucionar problemas en cuanto a seguridad de red, y así brindar un mejor servicio a los abonados del ISP.

Beneficios administradores.

- Capacidad de respuesta ante incidentes informáticos.
- Medidas preventivas y correctivas de seguridad.
- Capacidad de identificar intrusiones.

Beneficios para los usuarios.

- Disponibilidad del servicio de Internet.

4.4.3. Limitaciones y trabajos futuros.

El presente estudio identifica el tráfico malicioso en un escenario de infraestructura GPON en base a los scripts generados por la herramienta Snort, el cual es un IDS que permite la detección de intrusos. Para validar el funcionamiento se ejecuta el comando Hping3, el cual crea y analiza paquetes orientados a TCP/IP, sirve como testing de firewalls, escaneo de puertos y como un DDoS mediante un SYN Flood Attack.

En base a la investigación realizada se tiene que una red definida por software permite la mejora en los tiempos de conectividad y disminuye el procesamiento de los servidores físicos, lo que hace que trabaje de una manera eficaz. Esto se demuestra a través de pruebas de conectividad y pruebas de DDoS.

En este trabajo no se realizó un análisis estadístico de los resultados obtenidos, lo que se deja cómo propuesta para un futuro trabajo la realización de un análisis con el método wilcoxon, es una prueba no paramétrica para comparar el rango de medio de dos muestras relacionadas, el cuál analiza los datos recogidos por la investigación para evitar llegar a conclusiones erróneas.

Mitigar el ataque usando el controlador SDN, es una solución que se puede evaluar en futuros estudios ya que en este caso el controlador se convierte en un IPS bloqueando los ataques.

Se deja como propuesta la ejecución de ataques cibernéticos propios de las redes SDN, por ejemplo, se puede evaluar ataques como hampering el cual consisten en la modificación de la información de forma no autorizada del switch controlador o host, un ataque Hijacking el cual consiste en tomar el control de un elemento de red que en este caso puede ser del switch controlador o host. (DÁVILA, 2018)

CONCLUSIONES.

Se diseñó un sistema IDS en SDN para la prevención de ataques de seguridad (DoS), mediante el uso del controlador Ryu, el cual se encargó de realizar el encaminamiento de los paquetes desde su origen hasta el destino con la ayuda del protocolo OpenFlow.

Se investigó sobre los principales tipos de controladores que posiblemente puedan comunicar el IDS Snort con las redes SDN con Mininet, la cual se terminó que Ryu permite elaborar un conjunto de reglas precisas para ser incrustadas al sistema de detección de intrusos Snort con el fin de contrarrestarlos. entre los más destacados se encuentran los ataques por inundación mediante los protocolos ICMP, UDP y TCP.

Para comprobar la integración se realizó pruebas en dos escenarios, el primer escenario, fue realizar las pruebas pen testing a la red tradicional con IDS y determinar los tiempos de respuesta de los servicios, el segundo escenario fue realizar las mismas pruebas de pen testing implementado el IDS en las redes SDN. En el primer se detecta que los tiempos de respuesta del protocolo ICMP mejora con la implementación de una red SDN.

En las pruebas de funcionamiento del IDS en redes SDN se tiene una leve mejora en cuanto a los tiempos de respuesta de las alertas, lo más notorio es el nivel de CPU optimizando los recursos de procesamiento al momento de identificar tráfico malicioso.

Se realizó un análisis de costo beneficio justificando la necesidad de que los proveedores de Internet implementen esa solución y así incrementen sus niveles de seguridad en sus redes GPON, lo cual les permitirá brindar un buen servicio hacia los abonados.

RECOMENDACIONES.

Se recomienda que los sistemas utilizados en la implementación de los IDS en SDN sean actualizados y con la seguridad de Firewall necesarias para que funcionen correctamente, y a su vez logren detectar intrusos en el menor tiempo.

Es recomendable tener amplio conocimiento en uso de sistema operativo Linux, y así mismo sobre programación de las reglas del IDS Snort para comprender el funcionamiento de cada línea de código, pues si se modifica una mínima parte, el algoritmo realizara acciones diferentes a la deseada.

Se recomienda realizar un escenario virtual mediante la herramienta MiniNet integrada con GNS3, previo a la implementación de pruebas en un ambiente real, ya que esto puede afectar a la disponibilidad de los servicios del Proveedor de Internet.

Es recomendable comprender a su totalidad la composición de las reglas que se van a ejecutar en Snort, pues si se crea una sin un objetivo específico, puede no solo bloquear tráfico malicioso, sino también bloquear abonados que generan tráfico normal de su servicio.

Se recomienda realizar varias pruebas de funcionamiento en los diseños de red que permitan evaluar varios parámetros que validen de manera positiva o negativa si el proyecto ofrece un mejor servicio o si se debe desarrollar otra propuesta que se adapte a las necesidades tecnológicas.

REFERENCIAS

Pereira , G., & Gamess , E. (2017). Lineamientos para el Despliegue de Redes SDN/OpenFlow. *Revista Venezolana de Computación*.

Ali Ujjan, R., Pervez, Z., & Dahal, K. (2018). Suspicious Traffic Detection in SDN with. *IEEE*.

Calle, M., Tovar, J., Castaño, Y., & Cuéllar, J. (2018). Comparación de Parámetros para una Selección Apropiadade Herramientas de Simulación de Redes. *Información Tecnológica*.

Cervantes, M., Pesantez, D., Rosales, G., & Aranda, A. (2011). Diseño de seguridad en una Red GEPON orientada a servicios X-Play. *ESPOL*.

COIP. (2018). *Código Orgánico Penal .*

Coyla Jarita, Y. (2019). *UNIVERSIDAD PERUANA UNIÓNFACULTAD DE INGENIERÍA Y ARQUITECTURAEscuela Profesional de Ingeniería de SistemasImplementación deun sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguri.*

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2019). The ecology of trust among hackers. *Global Crime*.

E Tego, F. M. (2017). A Measurement Plane to Monitor and Manage QoS in Optical Access Networks.

E Tego, F. M. (2017). An Improved Algorithm for Querying Encrypted Data in the Cloud.

Espinosa , D., Martínez, J., & Siler, A. (2014). GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN CON BASE EN LA NORMA ISO/IEC 27005 DE 2011, PROPONIENDO UNA ADAPTACIÓN DE LA METODOLOGÍA OCTAVE-S. CASO DE ESTUDIO: PROCESO DE INSCRIPCIONES Y ADMISIONES EN LA DIVISIÓN DE ADMISIÓN REGISTRO Y CONTROL AC. *USBmed*.

FISCALIA GENERAL DEL ESTADO. (2019). 12 ataques por segundo se registran en Ecuador. *EL TELEGRAFO*.

Hendrawan, H., Sukarno, P., & Arief Nugroho, M. (2019). Quality of Service (QoS) Comparison Analysis of. *IEEE*.

Isaza. (2013). *Metodologías y Herramientas de Ethical Hacking.* Obtenido de https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

ISO. (2018). *ISO/IEC 27005.*

Keti, F., & Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. *IEEE*.

Loayza-Valarezo, P., Guaña-Moya, J., & Pumares-Romero, A. (2020). Guía metodológica de levantamiento de información para el diseño de redes FTTH-GPON con enfoque QoS. *RISTI*, 2.

M Diaa, M. S. (2018). Undetectable Tapping Methods for Gigabit Passive Optical Network (GPON).

Misaza. (2013). *Metodologías y Herramientas de Ethical Hacking* . Obtenido de https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

Mohammad Mousavi, S., & St-Hilaire, M. (2015). Early Detection of DDoS Attacks against SDN Controllers . *International Conference on Computing, Networking and Communications, Communications and Information SecuritySymposium*.

Nam, K., & Kim, K. (2018). A Study on SDN security enhancement using open. *IEEE Xplor*.

Ocampo, A. C., Castro Bermúdez , Y. V., & Solarte Martinez, G. R. (2017). Sistema de detección de intrusos en redes corporativas. *Scientia et Techinica XXII*.

(2017). *Plan Nacional de Desarrollo 2017-2021 Toda una Vida.*

Raza Shah, S., & Issac, B. (2018). *Performance comparison of intrusion detection systems and.* ScienceDirect.

Rodríguez-Fonseca*, A. A. (s.f.). Evaluation of QoS in RF/Li-Fi hybrid networks on 5th.

Salazar Hernández, R. (2016). *Sistema de Detección de Intrusos mediante modelado de URI.*

Sanchez Restrepo, S. J. (2017). *SISTEMA DE DETECCIÓN DE INTRUSOS MEDIANTE SNORT Y COMPARACIÓN CON OTRAS APLICACIONES.*

Skowyra, R., Bahargam, S., & Azer, B. (2016). 1Software-Defined IDS for Securing EmbeddedMobile Devices. *Computer Science Department*.

UNDRO. (1979). *Natural Disasters and Vulnerability Analysis.*

Valarezo, P. L., Moya, J. G., & Romero, A. P. (2019). Guía Metodológica de levantamiento de información para el diseño de redes FTTH-GPON con enfoque QoS. *Risti*.

W. Lee, S., Li, K.-Y., & Wu, M.-S. (s.f.). Design and Implementation of a GPON-based Virtual OpenFlow-enabled SDN Switch. *IEEE*.

ANEXOS

ANEXO 1. INSTALLING MININET ON CENTOS 7

OPERATING SYSTEM : CENTOS 7

PREREQUISITE : INSTALL EPEL REPOSITORY

(1) System Should be fully updated and Install gcc

yum update -y

yum install gcc* git

(2) Install the Python-pip

yum install python-pip -y

(3) Install python pyflakes

pip install pyflakes

(4) Install python Pexpect

pip install pexpect

(5) Install python nose

pip install nose

(5) Install python scapy

pip install scapy

(6) Download Mininet from github

git clone https://github.com/AOSL/MININET_CENTOS7.git

(7) Now Install The Mininet

cd MININET_CENTOS7

rpm -Uvh rdo-release.rpm

cd mininet/util

chmod 777 install.sh

util]# ./install.sh

[END OUTPUT}

make[1]: Nothing to be done for `install'.

make[1]: Leaving directory `/root/oflops/doc'

Enjoy Mininet!

(8) Start the openvswitch service and enable it

systemctl start openvswitch

systemctl enable openvswitch

(9) Run the Mininet from Terminal

mn

[OUTPUT]

*** Creating network

*** Adding controller

*** Adding hosts:

h1 h2

*** Adding switches:

s1

*** Adding links:

(h1, s1) (h2, s1)

*** Configuring hosts

h1 h2

*** Starting controller

c0

*** Starting 1 switches

s1 ...

*** Starting CLI:

mininet>

(10) Run the Wireshark and Select s1-eth1,s2-eh2 and press the start button

ANEXO 2. SERVIDOR PARA IMPLEMENTAR IDS EN SDN

The RackStation RS4021xs+ is powered by a 2.1 GHz Intel Xeon D-1541 Eight-Core processor, which will allow you to run multiple functions simultaneously. The built-in 16GB of DDR4 ECC RAM, which comes in a 1 x 16GB configuration, will allow quick access to frequently used files and programs and may also be upgraded to a total of 64GB by using a 16GB module in each of the four 288-pin DIMM slots. Also featured are two USB 3.2 Gen 1 Type-A ports, which allow it to be connected to external peripherals. Network connectivity is achieved via the two 10 Gigabit Ethernet or four Gigabit Ethernet ports with failover support, which help to provide redundancy in the case that a LAN connection malfunction occurs on one port. In addition, link aggregation helps to increase connection speeds beyond the limits of a single network port or cable. If you're looking to expand this NAS, there are two PCIe Gen 3.0 x8/x8 slots that support network interface cards and M.2 NVMe adapter cards for an SSD cache.

$ 5399.99

https://www.bhphotovideo.com/c/product/1618911-REG/synology_rackstation_rs4021xs_16_bay_nas.html/overview?gclid=EAIaIQobChMI7JbwyMan8wIVgeCzCh3yZAsmEAQYAiABEgLcfPD_BwE

ANEXO 3. PRECIOS DE LA EMPRESA SITEC