SISTEMA INTEGRAL PARA EL MONITOREO Y ANÁLISIS DE TRÁFICO DE UNA RED LOCAL

A SYSTEM FOR MONITORING AND TRAFFIC ANALYSIS IN A LOCAL NETWORK

Karen Lucero Roldán Serrato
Universidad Nacional Autónoma de México, Instituto de Ciencias Aplicadas y Tecnología, México
lucero.roldan@icat.unam.mx

Christian Rubén Obregón Sánchez
Universidad Nacional Autónoma de México, Instituto de Ciencias Aplicadas y Tecnología, México
christian.obregon@icat.unam.mx

Alethia Patricia Estrella Ruíz
Universidad Nacional Autónoma de México, Instituto de Ciencias Aplicadas y Tecnología, México
alethia.estrella@icat.unam.mx

Emmanuel Gómez Cantoya
Universidad Nacional Autónoma de México, Instituto de Ciencias Aplicadas y Tecnología, México
emmanuel.gomez@icat.unam.mx

Recepción: 30/octubre/2020 **Aceptación:** 27/noviembre/2020

Resumen

La optimización y seguridad del tráfico sobre una red datos se ha posicionado como prioridad en cuanto a la administración redes y la seguridad debido al incremento de dispositivos conectados a la red. En este trabajo se propone un sistema integral basado en herramientas de software para monitorear, analizar el tráfico de una red local y crear una estrategia de contención de amenazas a la actividad detectada sobre la infraestructura de TI (Tecnologías de Información). La importancia de este trabajo es la metodología mediante el análisis de paquetes basada en fragmentos de código o *scripts* de validación de estado para los equipos de red, así como la implementación de políticas de seguridad local. Los resultados de la metodología, aplicados al fortalecimiento de la seguridad en la red de datos, permiten una disminución del 18.47% en ataques e intrusiones por protocolos de acceso gracias al análisis numérico e identificación de patrones.

Palabras Claves: Análisis de tráfico, código de validación, contención de amenaza, monitoreo de red.

Abstract

The optimization and security of traffic over a data network have become a priority for network administration and security due to the increase in devices connected to the network. This work proposes a comprehensive system based on software tools for monitoring, traffic analysis of a local network and the creation a strategy to contain threats to the activity detected on the IT infrastructure (Information Technology). The importance of this work is the methodology through the analysis of packets based on code snippets or state validation scripts for network equipment, as well as the implementation of local security policies. The results of the methodology to strengthen security in the data network, 18.47% decrease in attacks and intrusions by access protocols, is achieved by numerical analysis and pattern identification.

Keywords: *Network monitoring, traffic analysis, threat containment, validation code.*

1. Introducción

Las recientes implementaciones tecnológicas sobre la administración de TI incluyen administración de redes, administración de sistemas, la seguridad de TI, la administración y asistencia de servicios y etc. El origen de un sistema de monitoreo y análisis de tráfico surgió de la necesidad de conocer las amenazas que existen ante la alta demanda de usuarios en la red. Se conoció que las fallas en la seguridad son causadas al menos tan a menudo por malos incentivos como por un mal diseño o baja priorización de la protección en la infraestructura de TI [Anderson, 2006].

A comienzos del siglo XXI y con el incremento de las redes empresariales bajo nuevas tecnologías sobre sus sistemas de sensores conectadas a internet se expuso una susceptibilidad a ciberataques [Song, 2012] [Mo, 2012]. Las contribuciones en los años siguientes se enfocaron en realizar un análisis de los niveles de la seguridad en los sistemas y se normalizó y adoptaron controles adecuados para reducir los riesgos de seguridad de acuerdo con la necesidad de la organización [Poolsappasit, 2012]. En la literatura se destacó la importancia del análisis de vulnerabilidad de seguridad en entornos de red, así como la aplicación de técnicas automatizadas de análisis de vulnerabilidad de archivos ejecutables, sobre métodos de localización de vulnerabilidades basadas en sistemas binarios y

en la extracción automática de las funciones relacionadas con la seguridad del *software* [Cheminod, 2013].

Por un lado, se propusieron modelos como gráficos de ataque, así como árboles de ataque para evaluar las relaciones causa-consecuencia entre los estados de la red, por otro lado, se exploraron diferentes formas para identificar la protección de la información para desarrollar un plan de gestión y mitigación de seguridad, mediante modelos de análisis dinámico de riesgos sobre la red, con el fin de proporcionar información al administrador de *TI* para toma de decisiones en un entorno con recursos limitados [Park, 2014].

Más tarde en temas de la seguridad de la información y debido a incidentes de ciberseguridad sobre datos e instituciones bancarias, así como la vulnerabilidad de la información que circula por la red, se proyectó el 2018 como un año atípico para México, los riesgos de amenazas de ataques cibernéticos se incrementan entre 40 y 50 por ciento, de acuerdo con los expertos de *TI*, tales como *Symantec*, *Axtel* y *Kroll* [Castañares, 2018]. Los datos reportados en las líneas de incidentes de Ciberseguridad en el año 2019 por parte de *CERT* (*Computer Emergency Response Team*), el centro de respuesta a incidentes de seguridad en tecnologías de la información confirmó que algunos ataques cibernéticos pueden afectar el rendimiento de hasta el 30% de la arquitectura, la pérdida de rendimiento existe, aunque varía bastante según la versión del sistema operativo y la plataforma *hardware* que utilicemos, para solucionar algunas vulnerabilidades es necesario el desarrollo de *software* para análisis de procesos y la adquisición de soluciones de seguridad que apoyen en la contención y mitigación de riesgos en la seguridad informática [Dawson, 2019]. Durante los meses del año 2019, los trabajos de la literatura reportaron sistemas de instrumentación basados en sistemas inteligentes con paradigmas de inteligencia artificial para detección de condiciones en los equipos de telecomunicaciones y en general las condiciones de los equipos distribuidores de red. Estos trabajos reportan las metodologías mediante sistemas de Control Distribuidos, llamada Arquitectura de malla, enfocada a sistemas de base de datos con escenarios previos y un sistema de comparación como reglas en un ambiente o sistema difuso (figura 1) [Berruti, 2019].

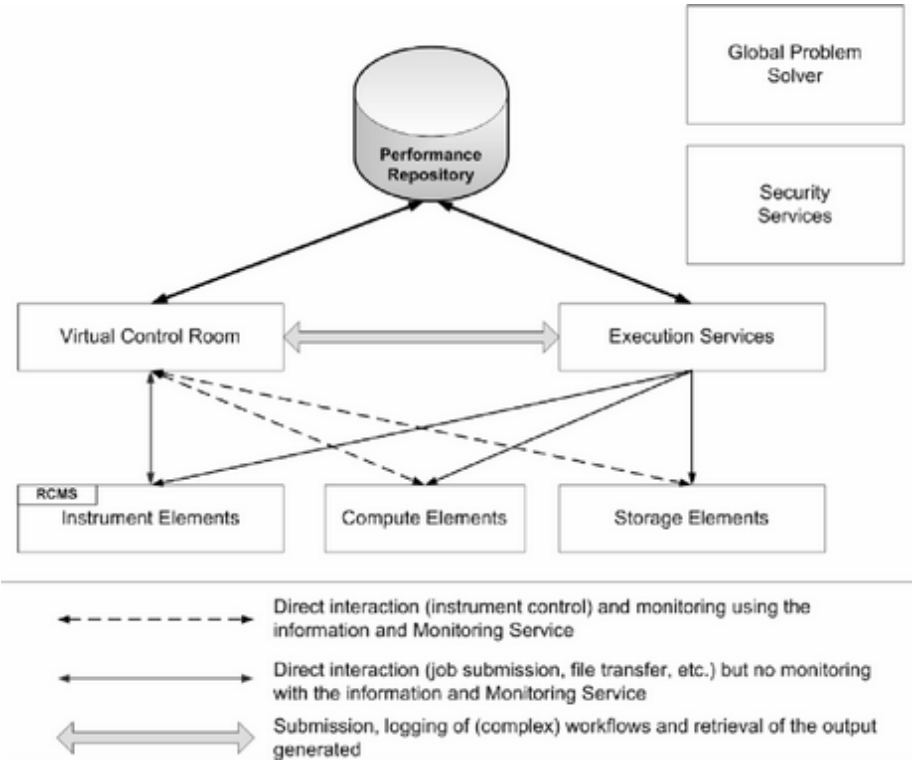


Figura 1 Sistema y arquitectura GRIDCC.

Así los sistemas de seguridad y análisis de control de tráfico pretenden tener una arquitectura definida con procesos de interacción sobre entradas y salidas para monitoreo de información y flujo de datos. Este trabajo es el complemento del análisis de tráfico mediante herramientas libres para la obtención de datos sobre los protocolos de comunicación y la obtención de muestreo mediante gráficos de tráfico (Roldán and et. al, 2019). La presente propuesta es la culminación con implementación del monitoreo de tráfico mediante fragmentos de código o *scripts* de validación de datos, así como el análisis numérico de los datos obtenidos y políticas de seguridad a la red de datos, con el fin de ofrecer un sistema integral de administración de red para la contención de amenazas en TI.

2. Métodos

El modelo de administración y gestión de la red de datos se basa en un conjunto de operaciones que nos permite administrar las tareas de la red, implica la coordinación de elementos orientados a funciones específicas. Ante las condiciones

de red no-configurables, el sistema integral de red aplicado a la ciberseguridad nos da un aporte de control a la red para que mantenga un ciclo continuo de planeación, implementación y validación y mejoras en el enlace de datos para el cumplimiento de estándares y protocolos de seguridad local y perimetral. La idea central de la metodología propuesta se basa en el análisis de paquetes sobre el desarrollo y creación de códigos o *scripts* de validación de estado para los equipos de red asociados a la activación de políticas de seguridad local, la figura 2 muestra un diagrama con las fases que contiene la metodología.

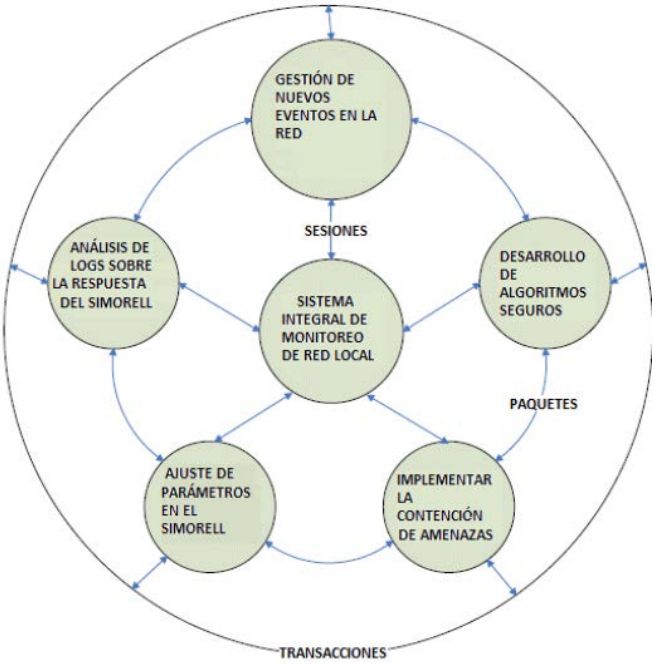


Figura 2 Sistema Integral de monitoreo y análisis de tráfico.

En la metodología se tienen algunas fases de desarrollo e implementación para la contención de amenazas, a continuación, se describen:

- Gestión de nuevos eventos en la red, permite el tráfico de los hosts conocidos, filtra cualquier conexión que no vaya a los puertos típicos usados en los servicios utilizados por el usuario o la conexión; en caso contrario, realiza el registro del evento sucedido en la red.
- Desarrollo de algoritmos seguros, el desarrollo a través de fragmentos de código o *scripts* basados en procesos de comportamiento de actividad

maliciosa o análisis de paquetes basados en el reconocimiento de patrones característicos nos permitirá proponer un módulo de aprendizaje y reconocimiento para la toma de decisiones de la siguiente etapa.

- Implementar la contención de amenazas, a través del análisis de vulnerabilidades en las sesiones, transacciones y en los paquetes de la conexión podemos crear acciones para reducir el efecto del ataque antes de llegar a la aplicación de políticas de seguridad y fortalecer el rendimiento del filtrado principal para reducir tiempo de respuesta.
- Ajuste de parámetros, según la respuesta del sistema dará la facultad de analizar los resultados de la implementación del sistema, así como eventos sucedidos por 24 horas y por semana con el fin de ajustar el proceso de contención de amenazas y mejorar los tiempos de respuesta y la configuración de los equipos asociados al sistema integral de monitoreo y análisis de tráfico.
- Análisis de *logs*, el análisis más detallado y un diagnóstico de la red, así como la mejora del proceso de reconocimiento de amenazas mediante la actividad histórica del *log* del uso de nuestra red.

En la última etapa del diagrama secuencial en la red de datos está basada en los mecanismos de administración de red respecto a la seguridad perimetral y local; este proceso incluye la creación y aplicación de políticas cuyas acciones de detección y contención de actividad de red en la capa de aplicación, así como la administración de los recursos de uso de la red mediante creación e implementación de políticas de seguridad directamente aplicadas al enlace de tráfico de entrada y salida de internet a las conexiones locales.

En el muestreo de tráfico de paquetes en la red de datos por ventana, se tiene el siguiente análisis de comportamiento, será el preámbulo para el desarrollo e implementación de los códigos de validación de paquetes (figura 3).

En el tráfico de datos se obtienen paquetes enviados y paquetes recibidos en proporción a un porcentaje de paquetes perdidos. Según el protocolo, se detectaron los niveles de refuerzo por horarios.

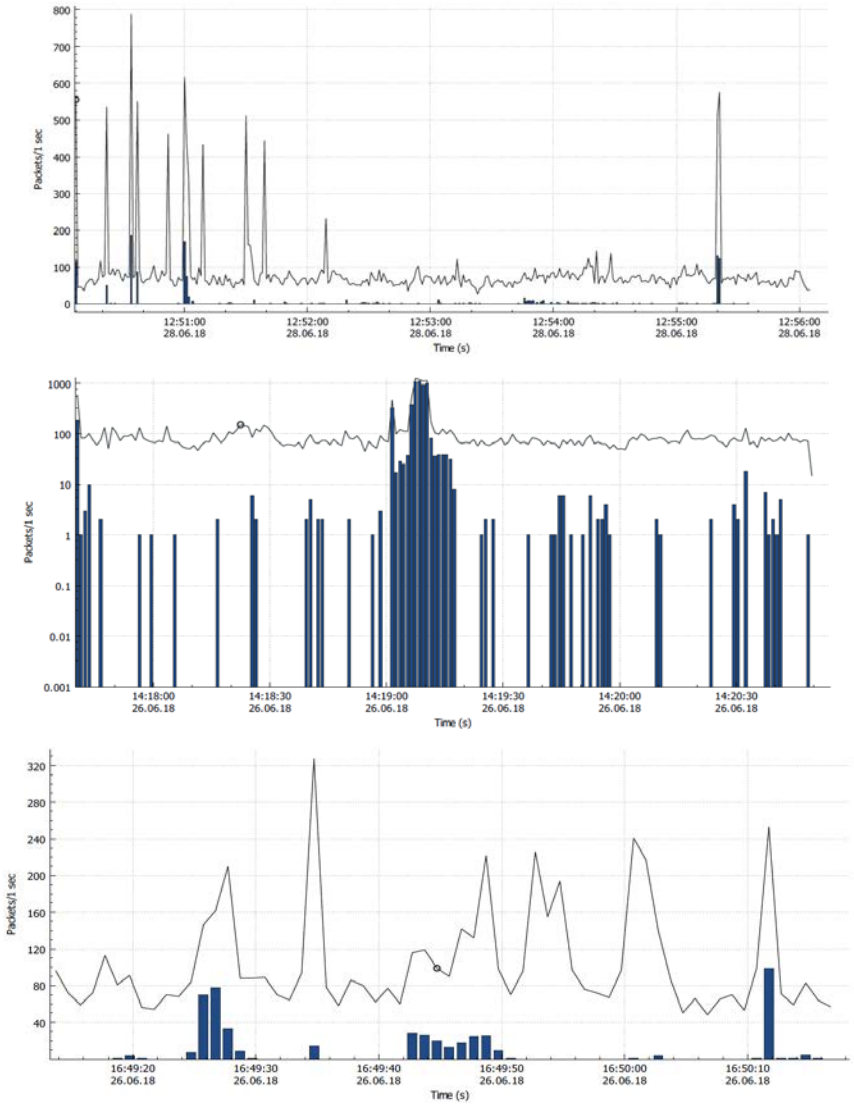


Figura 3 Muestreo de tráfico de paquetes.

Se presenta el pseudocódigo de los scripts asociados a la validación de estados de los paquetes enviados con los paquetes perdidos, para determinar patrones de comportamiento en los equipos de telecomunicaciones basados en lenguaje *sFlow* (lenguaje de programación libre asociado a los equipos de telecomunicaciones). La creación y la programación de scripts incluyen: un *script* de alerta de *log in* hacia el acceso a la red; un *script* de autenticación y envío de paquetes; un *script* de intercambio y desconexión de los equipos (recepción de paquetes) (figura 4). La aplicación de los *scripts* envía el *log* de los paquetes por correo, la estructura general se define mediante la siguiente tabla (tabla 1).

PSEUDOCÓDIGO SCRIPT DE ALERTA LOGIN

```
"result":{
 "domain":"auth (login)",
 "diag":400,
" e.msg": mylog@mydomain.mx
 "error":"Authentication failure: Invalid login name or
password","output":"",
 "data":[]}}
# Additional code goes here
 api.logout()
 except HTTPError, e:
 api.logout()
 print "Error: " + e.msg
```

SCRIPT DE AUTENTICACIÓN Y CONEXIÓN

```
function myvlans()
{
 echo -n "Enter VLAN id: "
 read vlanid
 if [ "$vlanid" -eq "" ]; do
"diag":read.packet(id.protocol.ident),
e:msg"send.message:read.packet","output":"",
" e.msg": mylog@mydomain.mx
 "
 "data":[]}}
 echo "No VLAN ID entered..."
 return 1
 fi
 vlan $vlanid
\
```

SCRIPT DE INTERCAMBIO Y DESCONEXIÓN

```
    "result":{
    "domain":"cli","cmd":"show
    vlan n",
    VLAN-1,\nType :
    Static Vlan,\nAdministrative
    State : enabled,\nOperational
    State : enabled,\nIP Router
    Port : enabled,\nIP MTU
    e:msg"received.message:send.packet","outp
ut":"","," e.msg": mylog@mydomain.mx
    "error":"
    ","data":[]}
     print "Error: " + e.msg
    }
```

Figura 4 Pseudocódigo de *scripts* de validación de tráfico de paquetes.

Tabla 1 Muestreo de *Log* por MAC del monitoreo de Red, de los dispositivos del ICAT.

“MACAddress","Packets","SendBytes", "ReceivedBytes", “Bytes”
"00:00:5e:00:01:08",656,39360,656,39360,0,0
"00:04:80:a0:40:00",33926,2043744,33926,2043744,0,0
"00:06:4f:37:b7:11",730,66973,730,66973,0,0
"00:13:3b:11:74:74",332,25392,307,23892,25,1500

En la última fase en la creación y la implementación de las políticas a través de la aplicación de *firewall* local en los sistemas operativos nativos que reciben el enlace de red (figura 5).

```
IPTABLES_MODULES="ip"

# Unload modules on restart and stop
#   Value: yes|no,  default: yes
# This option has to be 'yes' to get to a sane state for a firewall
# restart or stop. Only set to 'no' if there are problems unloading netfilter
# modules.
IPTABLES_MODULES_UNLOAD="yes"

# Save current firewall rules on stop.
#   Value: yes|no,  default: no
# Saves all firewall rules to /etc/sysconfig/iptables if firewall gets stopped
# (e.g. on system shutdown).
IPTABLES_SAVE_ON_STOP="no"

# Save current firewall rules on restart.
#   Value: yes|no,  default: no
# Saves all firewall rules to /etc/sysconfig/iptables if firewall gets
```

Figura 5 *Firewall* local mediante política de acceso y denegación de servicio.

En la última etapa de ajuste y validación de *log* para el ajuste del *firewall* local de los equipos asociados a la red, es un proceso que se basa desde la gestión de los parámetros en la red, la implementación de los códigos y la limitación de servicios mediante el análisis de paquetes.

En la aplicación de los scripts de validación de paquetes asociado al reporte del *firewall* perimetral sobre el análisis de intrusiones en la red (figura 6), se obtiene la información numérica de los eventos (ataques o amenazas).

Figura 6 *Log* de intrusión en firewall perimetral.

3. Resultados

De acuerdo con los objetivos iniciales que nos planteamos se realizó la evaluación del tráfico de paquetes en la red local, mediante los muestreos por horarios donde se presentaba mayor tráfico de paquetes (usuarios) en la red y se extrajeron gráficos y tablas para el análisis de los parámetros y validar el estado de la seguridad de las conexiones. Se realizó el filtrado de las transacciones por paquetes de envío y recepción para obtener el análisis de las fuentes de los

dispositivos conectados a la red. Mediante la programación de fragmentos de código, es decir mediante el desarrollo y programación de *scripts* de validación, los cuales contienen los procesos de la conexión, envío y recepción de paquetes hacia un *log* central, se logró la implementación y contención de actividad con ayuda de las políticas de seguridad en el *firewall* local y perimetral (figura 7).

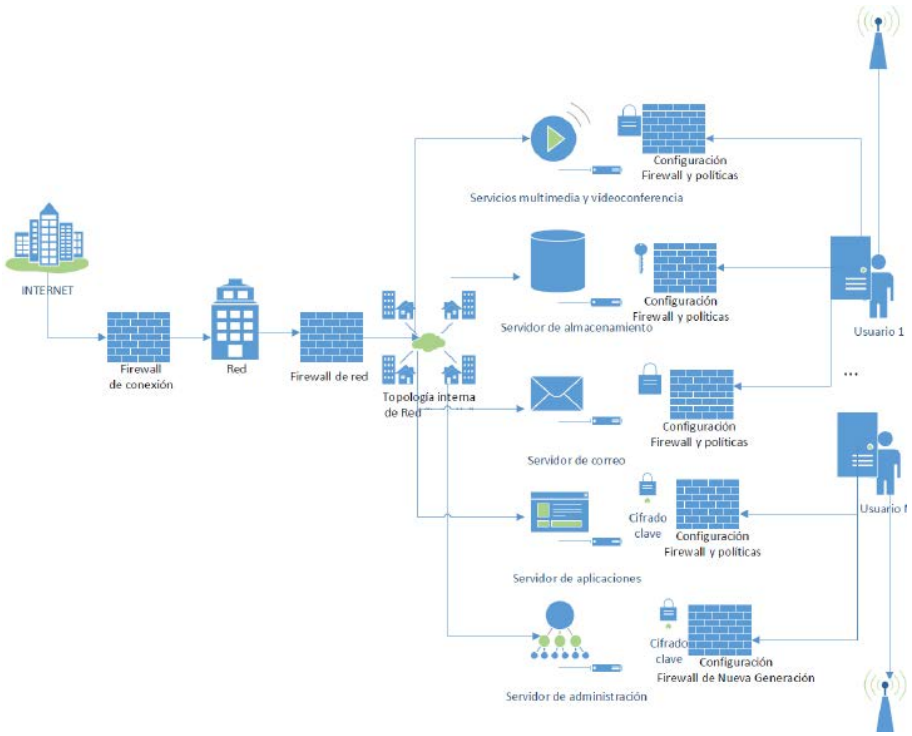


Figura 7 Infraestructura TI de contención de amenazas en una red local.

La creación de código de análisis que se crearon para la red local en estudio, a diferencia de otros algoritmos y protocolos de análisis propietarios, pueden demandar recursos de cómputo y análisis de tráfico innecesario, mientras que estos son hechos a la medida y demanda del tráfico de la red. Además, se creó la aplicación de políticas de seguridad a nivel *firewall* local y la validación del *log* de envío de los algoritmos y scripts se enviaron al correo electrónico de administración y al *log* del servidor de configuración de red (figura 8). La creación de los *scripts* en el análisis de paquetes fue un proceso fundamental en la metodología de análisis de tráfico local, mediante algoritmos de descifrado de tramas, es decir análisis de lo que contiene el paquete, de acuerdo con la terminación se determina la naturaleza

de la información. Este proceso es clave en un sistema auxiliar de detección de patrones que permita conocer mediante muestreos para no alterar el tráfico o flujo constante, en un futuro entrenar de forma artificial el sistema para mejorar el análisis de tráfico de la red local.

Figura 8 Validación de *log.*

Administración, configuración y permisos a usuarios en red

El monitoreo de red mediante muestreos de tiempo en la red de datos de la red local nos mostró un escenario inicial de conexiones y paquetes, respecto a la actividad de los usuarios como sus sesiones, protocolos, uso de ancho de banda y comunicación con la red local y con la aplicación de la metodología de detección de paquetes y aplicación de políticas se obtuvo la reducción de paquetes perdidos y paquetes maliciosos en la red del 18.47% (figura 9). Al inicio del análisis de tráfico de la red, el porcentaje de paquetes enviados es proporcional a los paquetes recibidos debido a que es un experimento controlado, con un flujo de datos determinado, con el fin de supervisar el algoritmo en producción a un sistema de red local expuesto a este tipo de muestreos.

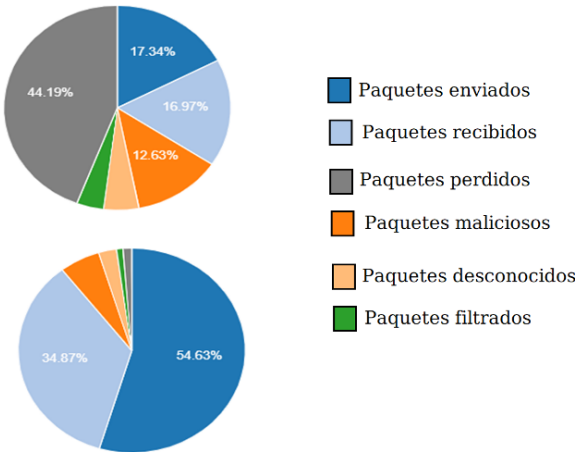
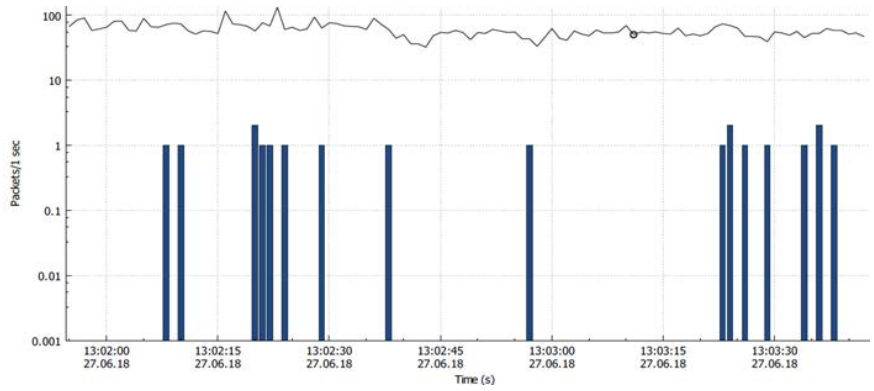


Figura 9 Porcentaje de paquetes identificados en la red.

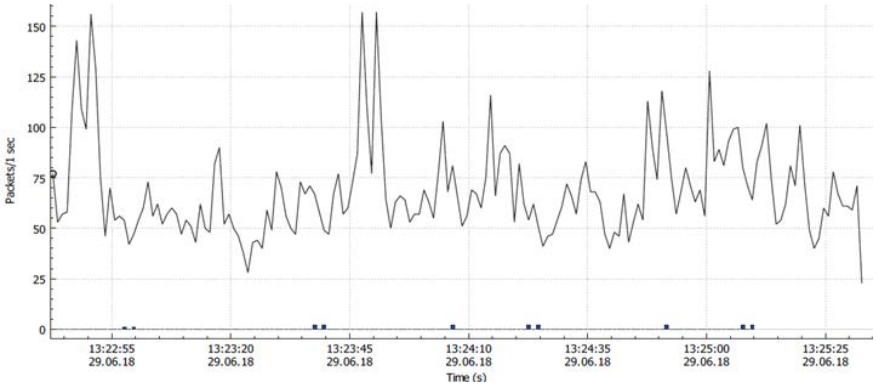
En la figura 9 segunda gráfica vemos un aumento en el porcentaje de paquetes enviados, así como paquetes recibidos y existe una clara disminución de paquetes maliciosos; debido a un análisis continuo y que el sistema va clasificando las reglas de los casos previos con los nuevos y puede realizar muestreos inmediatos.

4. Discusión

Se realizó una tabla comparativa con los datos de las gráficas iniciales sin la detección de paquetes, es decir con los muestreos iniciales de tráfico en la red y después de la implementación de los códigos de validación y aplicación de las políticas, se validaron los *logs (registros del sistema)* para tomar una métrica de comparación en los datos para medir los niveles de contención de paquetes maliciosos o perdidos. La comparación de gráfica de datos para los resultados inicial y final fue la base de nuestro estudio y la comprobación de la metodología de monitoreo y análisis de tráfico (figura 10).



a) Antes



b) Después

Figura 10 Identificación tráfico de paquetes.

La identificación del tráfico mediante la implementación del análisis de paquetes y la configuración de un firewall local es parte de la metodología clave para la reducción de actividad maliciosa en la red. Si se conoce el estado de los paquetes y si no se tiene un proceso que clasifique los mismos mediante políticas específicas no habría una disminución de amenazas y la red local estaría expuesta.

Mediante la implementación de *scripts* de control y análisis de tráfico en la red local se logra tener la base de una arquitectura segura y adaptable a las necesidades y tendencias de flujo de información.

5. Conclusiones

La aportación de este trabajo fue la implementación, configuración y administración de una metodología basada en algoritmos de validación de paquetes para la contención de amenazas en una red.

La importancia y relevancia también se basa en la implementación de herramientas de código implementadas en equipos de acceso, así como en los *firewalls* local y perimetral de la red, por las cualidades de administración, gestión, y aplicación de políticas de seguridad. Así como el uso controlado de las conexiones nos permite tener evidencias del alto consumo de nuestro enlace de datos por dispositivo y así tomarlo como antecedente en la mejora de la actividad maliciosa. Este trabajo permite crear una configuración lógica de nuestra red de datos y realizar el análisis de comparación logrando el 18% de mejora en la contención de paquetes maliciosos en la tarea de monitoreo en la administración de la infraestructura de TI.

6. Bibliografía y Referencias

[1] Anderson R., & Moore T., The economics of information security. science, no. 314:5799, 610-613, 2006.

[2] Cheminod M., Durante L., Valenzano A., Review of security issues in industrial networks, IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 277-293, 2013.

[3] Berruti L., Caviglione L., Davoli F., Polizzi M., Vignola S., Zappatore S., (2009). On The Integration of Telecommunication Measurement Devices

Within The Framework Of An Instrumentation Grid. In: Davoli F., Meyer N., Pugliese R., Zappatore S. (eds) Grid Enabled Remote Instrumentation.

[4] Signals and Communication Technology. Springer, New York, NY. Pp. 283-300, 2019.

[5] Castañares I., (2006). Elección dispara 50% el riesgo de ciberataques en México, dicen expertos. Recuperado el 30 de Mayo de 2020, de https://www.forbes.com.mx/hackers-roban-de-300-a-400-mdp-con-ataque-a-sistema-de-bancos/.

[6] Dawson M., Taveras P., Taylor D., Applying Software Assurance and Cybersecurity NICE Job Tasks through Secure Software Engineering Labs, Procedia Computer Science, vol. 164, 301-312, 2019.

[7] Mo Y., Kim T. H. J., Brancik K., Dickinson D., Lee H., Perrig A., Sinopoli B., Cyber-physical security of a smart grid infrastructure, Proceedings of the IEEE , vol. 100, no. 1, pp. 195-209, 2012.

[8] Park J., Suh Y., A development framework for software security in nuclear safety systems: integrating secure development and system security activities, Nuclear Engineering and Technology, vol. 46, no. 1, pp. 47-54, 2014.

[9] Poolsappasit N., Dewri R., Ray I., Dynamic security risk management using Bayesian attack graphs, IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, 2012.

[10] Roldan S. K. L., Estrella R. A. P., Arelio B. M. C., Gómez C. E., Domínguez R. O. D., Implementación de herramientas de *software* libre y análisis del monitoreo de red de datos como elemento primordial de la seguridad informática en un instituto. Congreso Internacional de emprendimiento sustentable y tecnológico para el desarrollo social y empresarial. Comitán Chiapas, México, 2019.

[11] Song J. G., Lee J. W., Lee C. K., Kwon K. C., Lee D. Y., A cyber security risk assessment for the design of I&C systems in nuclear power plants, Nuclear Engineering and Technology , vol. 44, no. 8, pp. 919-928, 2012.