Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

Tipo de artículo: Artículo original
Temática: Seguridad informática
Recibido: 16/02/2021 | Aceptado: 17/06/2021

Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red

Snort Open Source as intrusion detection for network infrastructure security

Hubner Janampa Patilla[1*] https://orcid.org/0000-0003-3110-194X
Hayde Luisa Huamani Santiago[2] https://orcid.org/ 0000-0002-8197-9956
Yudith Meneses Conislla[3] https://orcid.org/0000-0002-7646-5512

[1]Ingeniero Informático, Docente, Instituto de Investigación, Universidad Nacional de San Cristóbal de Huamanga, Perú. hubner.janampa@unsch.edu.pe
[2]Ingeniería de Sistemas, Universidad Nacional de San Cristóbal de Huamanga, Perú. hayde.huamani.27@unsch.edu.pe
[3]Ingeniería de Sistemas, Docente, Universidad Nacional de San Cristóbal de Huamanga, Perú. yudith.meneses@unsch.edu.pe

*Autor para la correspondencia. (hubner.janampa@unsch.edu.pe)

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

RESUMEN

Actualmente los ataques informáticos se han ido incrementando, afectando a diferentes empresas y organizaciones, a su vez ha provocado que los sistemas de detección de intrusiones sean requeridos en el esquema de seguridad de redes empresariales, esto debido a que los ataques informáticos son cada vez más elaborados y difíciles de detectar, un sistema de detección de intrusos en la red, mejora la detección de paquetes IP maliciosos, monitorea el tráfico de red entrante y saliente, identifica el uso no autorizado de las redes de los sistemas informáticos. Sin embargo, la mayoría de las Pymes no cuentan con este esquema de seguridad por diferentes motivos, entre ellas y la más importante, el costo que significa implementar un sistema de detección de intrusos. El objetivo de la investigación es de implementar Snort Open Source, como sistema de detección de intrusos para la seguridad de la infraestructura de red en entornos libres, aplicado a las Pymes. Para alcanzar los objetivos de la investigación, se utiliza la virtualización del sistema operativo GNU/Linux Ubuntu. A través de máquinas virtuales se implementa el escenario para llevar a cabo la configuración e implementación del Snort Open Source como sistema de detección de intrusos, para luego definir las reglas de filtrado para su funcionamiento.

Palabras clave. Snort Open Source; sistema de detección de intrusiones; pymes; ataques informáticos.

ABSTRACT

Currently, computer attacks have been increasing, affecting different companies and organizations, in turn, it has caused intrusion detection systems to be required in the corporate network security scheme, this due to the fact that computer attacks are increasingly Elaborate and difficult to detect, a network intrusion detection system, improves the detection of malicious IP packets, monitors incoming and outgoing network traffic, identifies unauthorized use of computer systems networks. However, most SMEs do not have this security scheme for different reasons, among them and the most important, the cost of implementing an intrusion detection system. The objective of the research is to implement Snort Open Source, as an intrusion detection system for the security of the network infrastructure in free environments, applied to SMEs. To achieve the research objectives, the virtualization of the GNU / Linux Ubuntu operating system is used. Through virtual

machines, the scenario is implemented to carry out the configuration and implementation of Snort Open Source as an intrusion detection system, and then define the filtering rules for its operation.

Keywords. Snort Open Source; intrusion detection system; pymes; computer attacks.

Introducción

Los riegos de la ciberseguridad en las Pymes son más frecuentes debido a que son empresas que están en crecimiento (Farro Flores, 2019). Los riesgos que hacen que una empresa sea vulnerable son las amenazas internas y externas, la infección por software malicioso y los ataques a nivel de red afectan al sistema de información (Francois Carpentier, 2016). Los diferentes tipos de ataques de los ciberdelincuentes no solo afectan a las grandes empresas, sino también a las pequeñas y medianas empresas, Pymes, y una de cada cinco de estas Pymes, son víctimas de ataques por ciberdelincuentes (Bardales, 2019).

El sistema de detección de intrusos, es un software, hardware o combinación de ambos que se utiliza para detectar la actividad de intrusos a nivel de red (Rehman, 2003). Para la detección de intrusos en la red, se utilizó herramientas inteligentes y automáticas para detectar intentos de intrusión en tiempo real (Arteaga, 2020), en concreto se implementó el Snort Open Source como IDS, esta es una herramienta de monitoreo y detección de primera línea (Thompson, 2020). El sistema de detección de intrusos implementado genera registros y alertas en tiempo real, y uno de los mayores problemas que tiene es con respecto a la administración del IDS, concretamente en el manejo del número potencial de grandes alertas y registros (Orebaugh, Biles & Babbin, 2005).

El sistema de detección de intrusiones se puede dividir en dos categorías: IDS basados en red, NIDS e IDS basados en host, HIDS. Ambos tipos de sistemas se pueden configurar para monitorear ataques, rastrear los movimientos de un pirata informático o alertar a un administrador sobre ataques en curso (Santos & Gregg, 2019). La tarea típica de los sistemas de detección de intrusos basado en red, NIDS, es el de identificar posibles patrones de ataque mediante el análisis del tráfico en red, procesando los paquetes de red en tránsito,

tanto los entrantes como los salientes (Parisi, 2019). NIDS intenta detectar actividades de red maliciosas, como, el de escaneo de puertos y ataques de denegación de servicios, DoS (Prowse, 2017). Los IDS tienen una visión gran angular de lo que está sucediendo dentro y alrededor de la red (Koziol, 2003). El sistema de detección de intrusos basados en host, HIDS, funciona con información recopilada dentro de un sistema informático individual y permite analizar las actividades con gran confiabilidad y precisión (Bace & Mell, 2015). El sistema de detección de intrusos distribuido, DIDS, funciona en una arquitectura Manager/Probe (realiza todas las operaciones de configuración en ubicaciones remotas), en donde los sensores de detección de NIDS se ubican de forma remota para informar a una estación de administración centralizada, que descarga las nuevas firmas de ataque a los sensores (Baker, Beale & Caswell, 2007).

Snort Open Source es un sistema de detección de intrusos en red, libre y gratuito. El sistema de detección de intrusiones basado en red, implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía en tiempo real (Costas Santos, 2014). Snort Open Source es un producto que combina la inspección basada en firmas y anomalías (Lane, Conklin, White & Williams, 2019). Snort realiza registros de paquetes en tiempo real, análisis de tráfico, análisis de protocolos y finalmente análisis de contenido (Goswami & Misra, 2017). Recopila información de una variedad de recursos del sistema y de la red, pero en realidad captura paquetes de datos según lo definido por la pila de protocolos TCP/IP (Vacca, 2012). Cada vez que un IDS basado en firmas localiza datos que coinciden con el contenido encontrado en una firma, genera datos de alerta para notificar a los analistas (Smith & Sanders, 2013). Snort trabaja a un nivel de detalle de escaneo de paquetes IP, y realiza la supervisión de la red a través de alertas basadas en eventos (Mandia, Luittgens & Pepe, 2014).

El trabajo principal de Snort es encontrar salidas de actividad de intrusión en paquetes con la ayuda de reglas, y si las encuentra se aplica la regla apropiada, de lo contrario descarta el paquete (Prakash & Kumar, 2012). Una regla de Snort tiene dos secciones: un encabezado y un cuerpo. El encabezado contiene la acción, el protocolo, las direcciones IP y las máscaras de red de origen y destino; mientras que el cuerpo contiene palabras clave que definen los criterios para activar una alerta (Woland, Kampanakis & Santos, 2016). Al detectar uno o varios tipos de actividad de intrusión genera alertas dependiendo de las veces que una regla haya coincidido con el contenido de un paquete (Rathaus, Ramirez, Caswell & Beale, 2005).

La motivación de realizar este trabajo de investigación respecto a la implementamos de Snort Open Source, se basa en que las Pymes que no cuentan con ningún tipo de seguridad frente a posibles ataques a nivel de red, y a través del IDS Snort Open Source, tenemos una solución para tomar medidas de seguridad a nivel de la capa de red. La implementación de Snort Open Source tiene como objetivo detectar las acciones que intentan comprometer la confidencialidad, disponibilidad e integridad de la información mediante la supervisión de los eventos que ocurren a nivel de red.

Método

Una vez que se realiza el análisis documental sobre los diferentes conceptos referentes al sistema de detección de intrusos a nivel de red Snort Open Source, se implementó un escenario con máquinas virtuales utilizando VM VirtualBox que un paquete de software de virtualización multiplataforma de código abierto (Dash, 2013), donde se realizaron las pruebas a cada una de las reglas implementadas, y se pudo verificar las alertas que emiten las reglas ante los posibles ataques.

Utilizamos la investigación aplicada para la implementación del IDS Snort, ya que con ella podemos actuar, transformar, modificar o producir cambios en un determinado sector de la realidad, para esta investigación es muy importante contar con el aporte de teorías científicas, que son producidas por la investigación básica y sustantiva (Carrasco, 2006).

Este trabajo de investigación es de tipo descriptivo, y nos permite especificar propiedades, características y perfiles importantes; una de las funciones principales de la investigación descriptiva es la capacidad para seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de dicho objeto (Hernández, Fernández & Baptista, 2010), en la presente investigación reflejamos este estudio descriptivo en la implementación del IDS Snort.

Resultados y discusión

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

Infraestructura de Red

Se elige una topología de red jerárquica, que nos permite agrupar equipos con funciones específicas, separándolo en tres niveles para facilitar el diseño, la implementación y su mantenimiento, esta topología nos permite que la red sea más confiable y escalable (Zheng, 2017). Este diseño de red LAN jerárquico incluye las siguientes tres capas (CISCO, 2014):

1. Capa de acceso: Que nos permite ofrecer a los terminales y usuarios el acceso directo a la red.
2. Capa de distribución: Que nos permite unir las capas de acceso y ofrecer conectividad a los servicios.
3. Capa central: Que nos permite ofrecer conectividad entre las capas de distribución para entornos de LAN grandes.

La estructura de red propuesta para las Pymes, está basada de acuerdo a las capas de diseño de red LAN jerárquico. Las diferentes áreas de la empresa cuentan con la misma topología y estructura de red.

Capa de acceso: Mostramos la topología estrella de cada una de las áreas funcionales de la Pyme, donde la conexión entre los diferentes dispositivos finales y el switch es de punto a punto.

Capa de distribución: En esta capa conectamos la capa de acceso con la capa de núcleo, y recibimos los datos de la capa de acceso antes de que se transmitan a la capa de núcleo, para su enrutamiento hacia su destino final, utilizamos el cable UTP y los conectores RJ-45.

Capa de núcleo: Esta capa es fundamental para la interconectividad entre los elementos de la capa de distribución y la capa de núcleo dentro de la arquitectura propuesta, que nos permite complementar el tráfico de todos los dispositivos de la capa de distribución, y reenviar grandes cantidades de datos para el enrutamiento hacia su destino final, también se utiliza el cableado UTP y conectores RJ-45, ver (Fig. 1).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

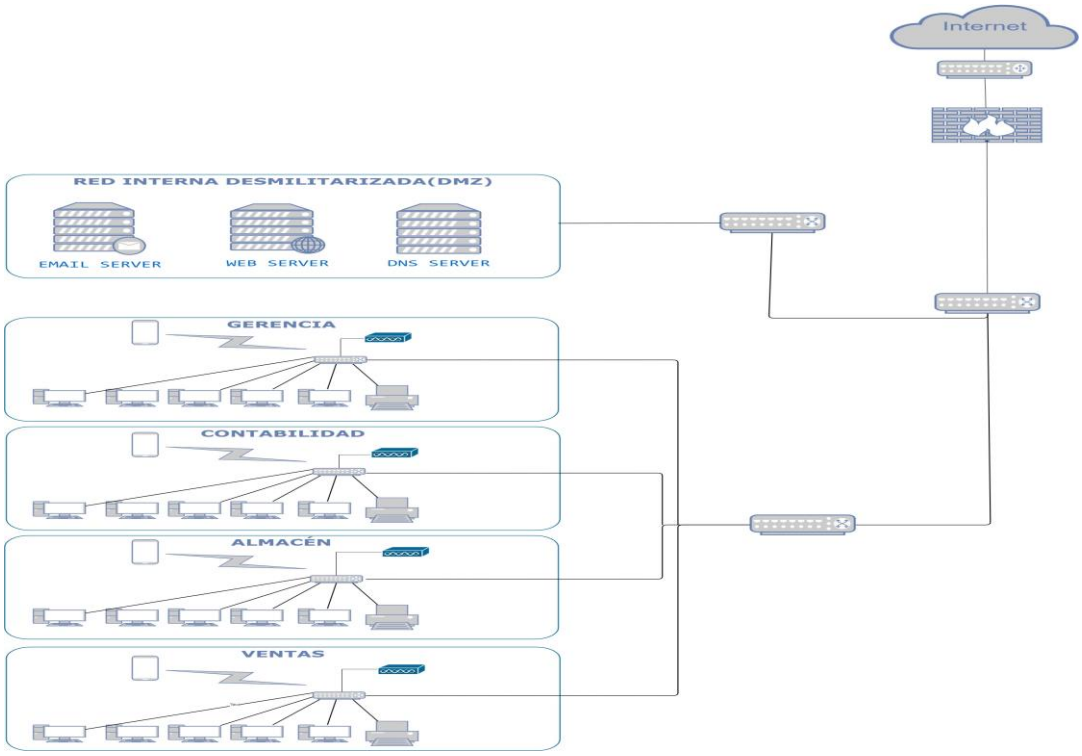

Fig. 1 – Estructura de red LAN Jerárquica propuesta para las Pymes.

¿Dónde colocar el sistema de detecciones de red Snort Open Source?

El lugar de ubicación de un IDS de red es importante, puesto que vigila todo el tráfico de red (Messier, 2019). Colocar el IDS detrás del cortafuego externo ofrece varias ventajas como la monitorizan intrusiones para los paquetes que logran atravesar el cortafuego principal, la detección de ataques a servidores, el reconocimiento de intentos de conexiones salientes, la identificación de ataques, el escaneo y monitorización de la red LAN; como sabemos muchas de las amenazas son provocadas por los usuarios internos al momento de ingresar a páginas no autorizadas (Arteaga, 2020). La zona de confianza es al inicio de la red LAN, donde se tiene una mayor sensibilidad, y cualquier tipo de alarma que se genere debe ser inmediatamente revisada ya que en esta zona los falsos positivos son muy pocos (Mira Alfaro, 2002), para la arquitectura propuesta de la topología de red para las Pymes utilizaremos este enfoque que acabamos de describir, es decir consideraremos la ubicación de nuestro IDS Snort después del cortafuego externo, ver (Fig. 2).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

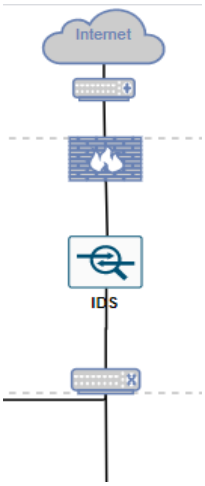

Fig. 2 – Estructura de red basada en sistema de detección de intrusiones a nivel de red, observar que el IDS Snort se coloca después del cortafuego externo.

Instalación y funcionamiento de Snort

Primero, nos aseguramos de que su sistema esté actualizado y tenga la última lista de paquetes mediante el siguiente comando:

```
>> sudo apt-get update && sudo apt-get dist-upgrade –y
```

Ahora verificamos que el sistema tenga la hora correcta y la zona horaria correcta. Esto será importante cuando comencemos a procesar alertas. El siguiente comando le permitirá elegir su zona horaria:

```
>> sudo dpkg-reconfigure tzdata
```

Ahora descargaremos varios archivos de origen con formato *tar* y otros archivos, crearemos las carpetas para almacenarlos:

```
>>mkdir ~/snort_src
>>cd ~/snort_src
```

Procedemos a la instalación bajo el siguiente comando:

```
>> sudo apt-get install snort
```

Snort informa sobre los intentos de intrusión detectados, realiza la detección y el análisis del tráfico de red (Blum & Bresnahan, 2020). Está basado en firmas, el IDS Snort tiene un archivo de firmas que enumera lo que se considera actividad sospechosa (Clarke, 2017).

Snort tienen dos partes lógicas: encabezado de regla y opciones de regla (Rehman, 2003). El encabezado de regla puede considerarse como una breve descripción de la conexión de red, donde cuatro parámetros definen una conexión de red única: IP de origen, puerto de origen, IP de destino y puerto de destino. Las opciones de regla definen lo que está involucrado en el paquete de red, básicamente es un mensaje a Snort para inspeccionar el paquete en busca de valores coincidentes y determinar si se considera malicioso el paquete (Cox & Gerg, 2004).

Recordar además que TCP como protocolo orientado a la conexión, transfiere datos entre dispositivos (Gordon, 2019). UDP es un protocolo de capa de transporte simple, orientado a datagramas que preserva los límites de los mensajes (Stevens & Fall, 2011), en la (Fig. 3) se muestra la estructura de las reglas Snort.

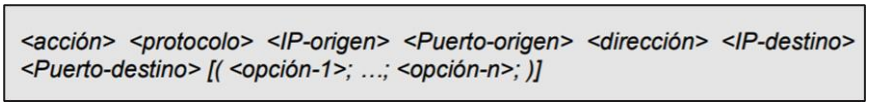

Fig. 3 – Estructura de reglas Snort (De Haro Bermejo, 2015).

Las reglas que se definen en el motor de detección serán colocadas en el directorio de local.rules. Cuando se envían datos a la red, primero va al servidor donde se ejecuta Snort para analizar y buscar contenido malicioso en los paquetes (Sharma, Kumar & Tasneem, 2018).

La variable **HOME_NET** define las direcciones de red a monitorear. Asimismo, la variable **EXTERNAL_NET** define qué hosts externos monitorear. El valor predeterminado **ANY** permite monitorear todas las direcciones de red local, ver tabla1.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

Tabla 1 - Reglas para el motor de detección Snort.

ALERTA	PROTOCOLO	DIRECCION ORIGEN	DIRECCION DESTINO	PUERTO ORIGEN	PUERTO DESTINO
Prueba ICMP detectada	IMCP	any	HOME_NET	any	any
Escaneo de puertos TCP detectada	TCP	any	HOME_NET	any	any
Intento de conexión FTP	TCP	any	HOME_NET	any	21
Intento de conexión TELNET	TCP	any	HOME_NET	any	80
Posible ataque DoS TCP	TCP	any	HOME_NET	any	80
Conexión SSH detectada	TCP	any	10.0.2.15	any	22
Alerta de ingreso a Facebook	TCP	any	HOME_NET	any	any
Alerta de ingreso a Youtube	TCP	any	HOME_NET	any	any

Configuración y ejecución de las reglas Snort

Antes de configurar las reglas, tenemos que ejecutar Snort en modo Sistema de Detección de Intrusos a nivel de red (NIDS) tal como se muestra en (Fig. 4).

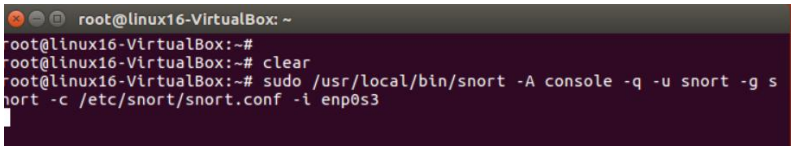

Fig. 4 – Snort en modo NIDS.

1. **ICMP detectada**: Esta regla genera una alerta, con un comportamiento sospechoso en el protocolo **ICMP** desde cualquier dirección IP de origen y puerto origen. Teniendo como dirección de IP destino **$HOME_NET**, que ingresa por cualquiera de los puertos. El mensaje que emite la alerta en el IDS Snort es “Prueba ICMP detectada”, ver (Fig. 5).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

Regla implementada Snort:

alert icmp any any -> $HOME_NET any (msg:"Prueba ICMP detectada"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

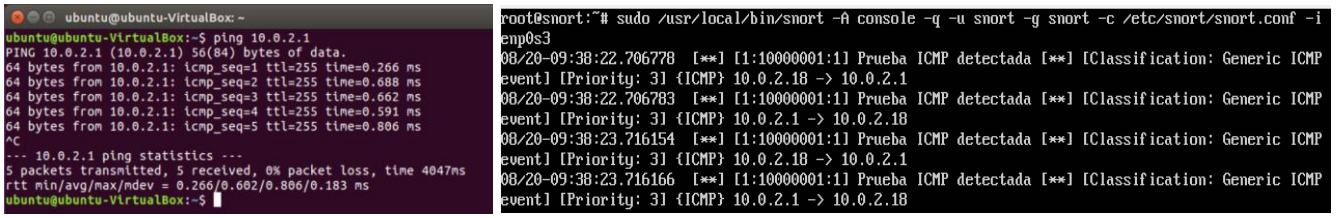

Fig. 5 – Prueba de regla ICMP.

2. **Escaneo de puertos TCP**: La regla genera una alerta, con un comportamiento sospechoso en el protocolo TCP desde cualquier dirección IP de origen y puerto origen. Teniendo como dirección de IP destino $HOME_NET, que ingresa por cualquiera de los puertos. El mensaje que emite la alerta en el IDS Snort es “Escaneo de puertos TCP detectada”, ver (Fig. 6).

Regla implementada Snort:

alert tcp any any -> $HOME_NET any (msg: “Escaneo de puertos TCP detectada”; GID:1; sid:10000002; rev:001; classtype:web-application-attack; detection_fi ter:track by_src, count 30, seconds 60;)

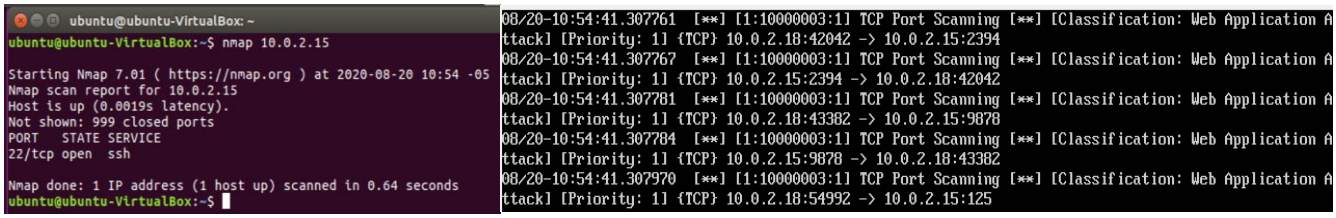

Fig. 6 – Prueba de regla escaneo de puertos TCP.

3. **Intento de conexión FTP**: La regla genera una alerta, con un comportamiento sospechoso en el protocolo TCP desde cualquier dirección IP de origen y puerto origen. Tiene como dirección de IP destino **$HOME_NET** y puerto de destino 21, el mensaje que emite la alerta en el IDS Snort es “Intento de conexión FTP”, ver (Fig. 7).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

Regla implementada Snort:

alert tcp any any -> $HOME_NET 21 (msg:"Intento de conexión FTP sid:10000003; rev:001;)

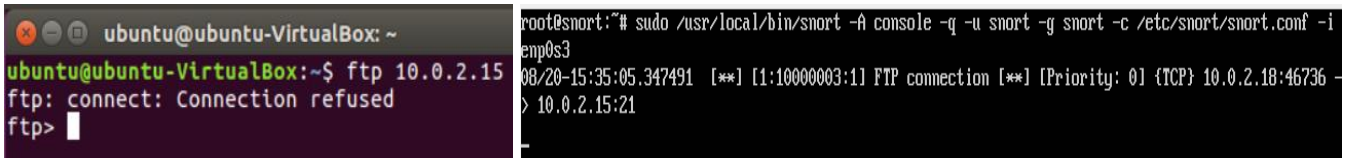

Fig. 7 – Prueba de regla intento de conexión FTP.

4. **Intento de conexión TELNET**: La regla genera una alerta, con un comportamiento sospechoso en el protocolo TCP desde cualquier dirección IP de origen y puerto origen. Tiene como dirección de IP destino $HOME_NET y puerto de destino 80. El mensaje que emite la alerta en el IDS Snort es "Intento de conexión TELNET", ver (Fig. 8).

Regla implementada Snort:

alert tcp any any -> $HOME_NET 80 (msg:" Intento de conexión TELNET"; sid:10000004; rev:001;)

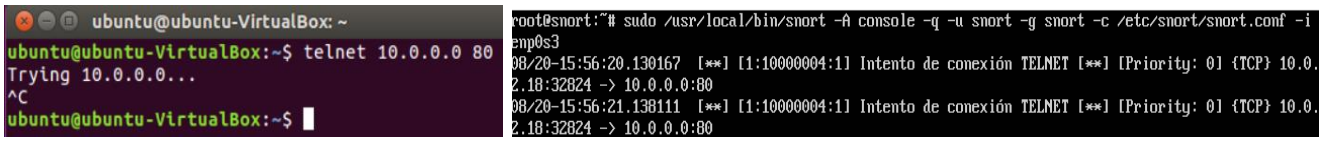

Fig. 8 – Prueba de Regla Intento de conexión TELNET.

5. **Posible ataque DoS TCP**: La regla genera una alerta ataque de denegación de servicio distribuido, con un comportamiento sospechoso en el protocolo TCP desde cualquier dirección IP de origen y puerto origen. Tiene como dirección de IP destino $HOME_NET y puerto de destino 80. El mensaje que emite la alerta en el IDS Snort es "Posible TCP DoS", ver (Fig. 9).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

Regla implementada Snort:

alert tcp any any -> $HOME_NET 80 (flags: S; msg “Possible TCP DoS;Flow:stateless; threshold: type both, track by_src, count 70, seconds 10; sid:10000005;rev:001;)

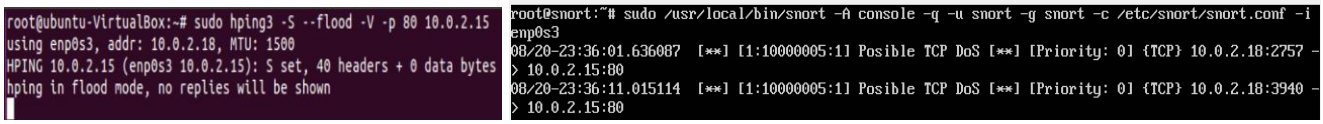

Fig. 9 – Prueba de regla posible ataque DoS distribuido TCP.

6. La regla genera una alerta de una conexión no permitida de **SSH**, esta regla tiene un comportamiento sospechoso en el protocolo TCP desde cualquier dirección IP de origen y puerto origen. Tiene como dirección de IP destino 10.0.2.15 y puerto de destino 22. El mensaje que emite la alerta en el IDS Snort es “Conexión SSH detectada”, para verificar la regla anterior utilizaremos la herramienta PuTTY desde donde podemos conectarnos a servidores remotos, ingresando el nombre o dirección IP del host y puerto, ver (Fig. 10).

Regla implementada Snort:

alert tcp any any -> 10.0.2.15 22 (msg: “Conexión SSH detectetada”; sid:10000006;)

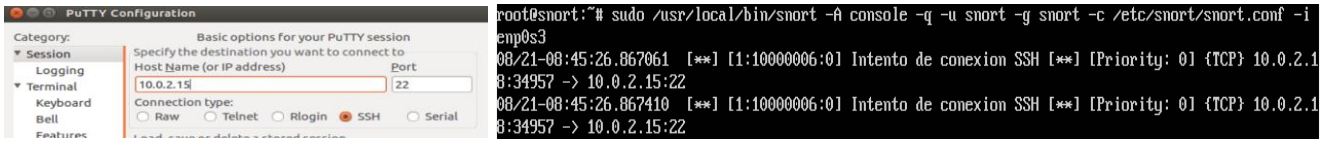

Fig. 10 – Prueba de regla conexión SSH a través de una herramienta PuTTY.

7. Alerta de ingreso a Facebook: La regla genera una alerta de una conexión a Facebook, esta regla tiene un comportamiento sospechoso en el protocolo TCP desde cualquier dirección IP de origen y puerto origen. Tiene como dirección de IP destino **$HOME_NET** y puerto de destino **ANY**. El mensaje que emite la alerta en el IDS Snort es “Alguien se encuentra ingresando a Facebook”, ver (Fig. 11).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. 3, Julio-Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 55-73

Regla implementada Snort:

alert tcp any any -> $HOME_NET any (content: “www.facebook.com”; msg:” Alguien se encuentra ingresando a Facebook”; sid:10000007; rev:001;)

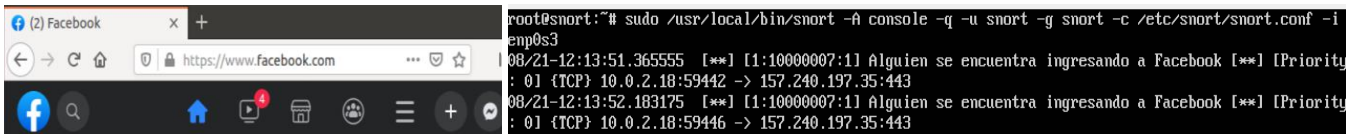

Fig. 11 – Prueba de regla ingreso a Facebook.

8. Alerta de ingreso a YouTube: La regla genera una alerta de una conexión a YouTube, esta regla tiene un comportamiento sospechoso en el protocolo TCP desde cualquier dirección IP de origen y puerto origen. Tiene como dirección de IP destino **$HOME_NET** y puerto de destino **ANY**. El mensaje que emite la alerta en el IDS Snort es “Alguien se encuentra ingresando a YouTube”, ver (Fig. 12).

Regla implementada Snort:

alert tcp any any -> $HOME_NET any (content: “www.youtube.com”; msg:” Alguien se encuentra ingresando a youtube”; sid:10000008; rev:001;)

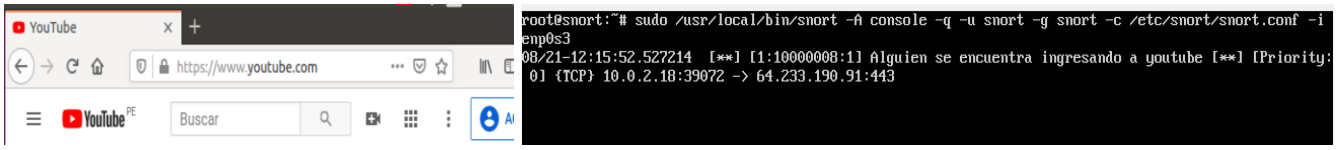

Fig. 12 – Prueba de regla ingreso a YouTube.

Conclusiones

Se puede afirmar que a lo largo de la investigación se logró implementar y mostrar la utilidad del sistema de detección de intrusos Snort con respecto a la seguridad de la infraestructura a nivel de red para una Pyme. Al monitorear el tráfico de red y realizar las pruebas necesarias se muestra el resultado como solución para una buena seguridad de la red de filtrado de paquetes.

Se implementó el diseño de la estructura de red para las Pymes basada en el sistema de detección de intrusos Snort, se identificó el lugar adecuado para su implementación, y desde donde se logró detectar con éxito el tráfico de la red entrante para la Pyme, además de monitorear el tráfico autorizado y no autorizado; asimismo esto nos permite estar alerta frente a cualquier tipo de incidente que se pudiera presentar cuando se quiere vulnerar la infraestructura de red de las Pymes.

Se logró realizar la implementación de Snort como un método de captura de paquetes, para que al momento en que circula un paquete por la red, este sea capturado por el módulo DAQ (Data Acquisition library), que lo reenvía posteriormente a Snort, este lo analiza a través del sistema de detección de intrusos a nivel de red.

Se logró implementar reglas de filtrado en el motor de reglas de Snort, y se realizó el filtrado de eventos y vulnerabilidades, estas reglas alertan los posibles intentos de ataques como la denegación de servicios, ingresos a páginas no autorizadas, escaneo de puertos entre otros. Se logró verificar que dichas reglas implementadas cumplen con su propósito, puesto que se realizaron las pruebas necesarias para garantizar que la misma cuenta con la funcionalidad esperada.

Referencias

Arteaga, J. E. Evaluation of the functionalities of the intrusion detection systems based on the network of open source platforms using the anomaly detection technique. Latin-American Journal of Computing (LAJC), 2020, 7(1): p. 49-64.

Bace, R. and Mell, P. Intrusion Detection Systems, NIST Special Publication on Intrusion Detection System, 2015, 3: p. 1-51.

Bardales, E. Diario Gestión [En línea]. Una de cada cinco pymes es víctima de delitos cibernéticos, según Microsoft. 2014, [Consultado el: 5 de Julio de 2020]. Disponible en https://gestion.pe/tecnologia/cinco-pymes-victima-delitos-ciberneticos-microsoft-73780-noticia/?ref=gesr.

Baker, A., Beale, J. and Caswell, B. J. Open Source Security Series Snort IDS and IPS Toolkit. Burlington: SYNGRESS, 2007, p. 19.

Blum, R. and Bresnahan, C. Study Guide LPIC-2: Linux Professional Institute Certification Study Guide, 2nd Edition. Estados Unidos: Sybex, 2016, p. 103-106.

Carrasco, S. Metodología de la Investigación Científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación. Lima: San Marcos, 2006, p. 44.

CISCO. Diseño de red LAN cableada [En línea]. Estructura de red LAN jerárquica, [Consultado el: 18 de Julio de 2020]. Disponible en https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf.

Clarke, G. E. Certification Study Guide, Third Edition (Exam SY0-501), 3rd Edition. Estados Unidos: McGraw-Hill, 2017, p. 81-83.

Costas Santos, J. Ciclos Formativos. Seguridad y Alta Disponibilidad. España: RA-MA, 2014, p. 139.

Cox, K. and Gerg, C. Intrusion Detection with Open Source Tools Managing Security with Snort & IDS Tools. Canada: O'Reilly Media, 2004, p. 33-36.

Dash, P. Getting Started with Oracle VM VirtualBox. Build your own virtual environment from scratch using VirtualBox. Reino Unido: Packt Publishing, 2013, p. 12.

De Haro Bermejo, F. Detección de intrusiones con Snort. Tesis de Posgrado Seguridad de Redes y Sistemas, Universitat Oberta de Catalunya, Catalunya, 2015.

Farro Flores, C. Uno de los activos más importantes del negocio es la información. Ciberdelincuencia: Amenaza Latente, 2019, 38: p.11-12.

Francois Carpentier, J. La seguridad informática en la PYME. Situación actual y mejores prácticas. Barcelona: Ediciones ENI, 2016, p. 427.

Gordon, D. Networking Fundamentals Develop the networking skills required to pass the Microsoft MTA Networking Fundamentals Exam. Reino Unido: Packt, 2019, p. 18.

Goswami, S. and MISRA, S. Network Routing Fundamentals, Applications, and Emerging Technologies. Reino Unido: Wiley, 2017, p. 42.

Hernández, R., Fernández, C. and Baptista, M. Metodología de la Investigación. En: Mares, J. (Editor). Definición del alcance de la investigación a realizar: exploratoria, descriptiva, correlacional o explicativa. Mexico: The McGraw-Hill, 2010, p. 80.

Koziol, J. Intrusion Detection with Snort. Estados Unidos: Sams, 2003, p. 21.

Lane, N., Conklin, W. A., White, G. B. and Williams, D. Certification All-in-One Exam Guide, Second Edition (Exam CAS-003). Estados Unidos: McGraw-Hill, 2019, p. 62-64.

Mandia, K., Luttgens, J. and PEPE, M. Incident Response & Computer Forensics. Estados Unidos: McGraw-Hill, Third Edition, 2014, p. 39.

Messier, R. C. Certified Ethical Hacker Study Guide. Canadá: Sybex, 2019, p. 73.

Mira Alfaro, E. J. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Tesis Licenciatura en Ingeniería Informática. Universidad de Valencia, Valencia, 2002.

Orebaugh, A., Biles, S. and Babbin, J. Solutions and Examples for Snort Administrators. En: Randal, A. y Apandi, T. (Editores). Snort Cookbook Solutions and Examples for Snort Administrators. Estados Unidos: O'Reilly & Associates, 2005, p. 32-37.

Parisi, A. Artificial Intelligence for Cybersecurity. Reino Unido: Packt Publishing, 2019, p. 46.

Prakash, O. and Kumar, V. International Journal of Computer Applications & Information Technology. Signature Based Intrusion Detection System Using SNORT, 2012, 1(3): pp. 35-41.

Prowse, D. L. CompTIA® Security+ SY0-501 Cert Guide. Estados Unidos: PEARSON, 2017, p. 54.

Rathaus, N., Ramirez, G., Caswell, B. and BEALE, J. Nessus, Snort, and Ethereal Power Tools Customizing Open Source Security Applications. Estados Unidos: Syngress, 2005, p. 29-33.

Rehman, R. B. Intrusion Detection With Snort, Apache, MySQL, PHP, And ACID. Estados Unidos: Pearson Technology Group, 2003, p. 10-12.

Santos, O and Gregg, M. Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd Edition. Estados Unidos: Pearson IT Certification, 2019, p. 211.

Sharma, S., Kumar, A. and TASNEEM, A. International Journal of Computer Applications. Intrusion Detection Prevention System using SNORT, 2018, 181(32): p. 21-24.

Smith, J. Y Sanders, C. Applied Network Security Monitoring. Estados Unidos: Syngress, 2013, p. 42.

Stevens, W. R. and Fall, K. R. TCP/IP Illustrated, Volume 1. En: Wait, J. The Protocols. Estados Unidos: Addison-Wesley Professional, 2011, p. 41.

Thompson, E. C. Guide to Detecting and Responding to Healthcare Breaches and Events. Estados Unidos: Apress, 2020, p. 23.

Vacca, J. R. Handbook computer and information security, 2nd edition. Estados unidos: elsevier, 2012, p. 51-52.

woland, A., Kampanakis, P. and Santos, O. Cisco Next-Generation Security Solutions. All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Singapur: Cisco Press, 2016, p. 59-60.

Zheng, L. P. Diseño e Implementación de una Red LAN para la Empresa Palinda. Tesis de Licenciatura en Redes y Sistemas Operativos. Universidad San Francisco de Quito, Quito, 2017.

Conflicto de interés

No existe conflicto de interés de este trabajo con ninguna organización académica y/o comercial y autorizan la distribución y uso del artículo.

Contribuciones de los autores

1. Conceptualización: Hubner Janampa Patilla.
2. Curación de datos: Hubner Janampa Patilla.
3. Análisis formal: Hayde Luisa Huamani Santiago, Yudith Meneses Conislla.
4. Adquisición de fondos: Hubner Janampa Patilla.
5. Investigación: Hubner Janampa Patilla.
6. Metodología: Hubner Janampa Patilla.
7. Administración del proyecto: Hayde Luisa Huamani Santiago.
8. Recursos: Hayde Luisa Huamani Santiago.
9. Software: Hayde Luisa Huamani Santiago.
10. Supervisión: Hubner Janampa Patilla.
11. Validación: Yudith Meneses Conislla
12. Visualización: Hubner Janampa Patilla.
13. Redacción – borrador original: Yudith Meneses Conislla.

14. Redacción – revisión y edición: Yudith Meneses Conislla.

Financiación

No se obtuvo financiamiento por parte de ninguna institución académica y/o comercial para realizar este trabajo de investigación.