
**UNIVERSIDAD TÉCNICA DE BABAHOYO**

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**

**PROCESO DE TITULACIÓN**

**NOVIEMBRE 2021 - ABRIL 2022**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRÁCTICA PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS**

**TEMA:**

# ANÁLISIS COMPARATIVO SOBRE LAS HERRAMIENTAS DE SEGURIDAD INFORMÁTICA OPEN SOURCE: NESSUS Y SNORT

**EGRESADO(A):**

**MARIA BRIGITTE MOSQUERA MAZACON**

**TUTOR:**

**ING. MIGUEL ANGEL ZUÑIGA SANCHEZ**

**BABAHOYO – ECUADOR**

**AÑO 2022**

**TEMA:**

# ANÁLISIS COMPARATIVO SOBRE LAS HERRAMIENTAS DE SEGURIDAD INFORMÁTICA OPEN SOURCE: NESSUS Y SNORT

**Resumen.**

Actualmente, son muchas las empresas que tienen información almacenada en sistemas informáticos o en nubes, de allí nace la necesidad de la empresa de proteger las bases de datos y equipos de los ataques o intrusos, lo cual es relevante tanto para la actividad de esta, como para su reputación. Y es por ello que le prestan atención a la seguridad informática o ciberseguridad. La seguridad informática acciona diferentes mecanismos con el fin de resolver un problema que se presente ante los equipos informáticos debido a las intrusiones o por el mal uso por parte de la persona que lo maneja, ya sea de forma involuntaria o intencionada.

Los ataques informáticos son un gran problema para las empresas, ya que ponen en riesgo su información confidencial y los obligan a gastar millones de dólares para recuperar el control de sus sistemas y datos. Generar un plan de seguridad informática es imprescindible para cualquier organización. Esto les permitirá a las empresas detectar vulnerabilidades en sus sistemas y establecer medidas para prevenir ataques. El objetivo es que ayude a proteger los datos y sistemas críticos del negocio.

Trabajar en reforzar la seguridad informática de un negocio se convierte en uno de los procesos fundamentales para que las empresas puedan garantizar el buen rendimiento de la misma. Para ello es importante conocer a fondo las principales herramientas de seguridad informática y, sobre todo, saber cuáles son aquellas que se encuentran más recomendadas y en forma a lo largo del periodo actual.

**Palabras claves.**

Seguridad informática, ciberdelincuentes, herramientas de seguridad

**Summary.**

Currently, there are many companies that have a lot of information stored in computer systems or in clouds (clouds), hence the need for the company to protect databases and equipment from attacks or intruders, which is relevant both for the activity of this, as for its reputation. And that is why they pay attention to computer security or cybersecurity. Computer security activates different mechanisms in order to solve a problem that arises before computer equipment due to intrusions or misuse by the person who handles it, either involuntarily or intentionally.

Cyber attacks are a huge problem for businesses, putting their sensitive information at risk and forcing them to spend millions of dollars to regain control of their systems and data. Generating a computer security plan is essential for any organization. This will allow companies to detect vulnerabilities in their systems and establish measures to prevent attacks. The goal is to help protect critical business data and systems.

Working to reinforce the computer security of a business becomes one of the fundamental processes for companies to guarantee its good performance. For this, it is important to know in depth the main computer security tools and, above all, to know which are those that are most recommended and in shape throughout the current period.

**Keywords:**

Informatic security, cyber criminals, security tools

**Introducción.**

En la actualidad la tecnología podría referirse como la colección de herramientas lo cual pueden hacer más sencillo usar, crear, administrar e intercambiar información. Es el conocimiento y utilización de herramientas, técnicas y sistemas con el fin de servir a un propósito más grande como la resolución de problemas o hacer la vida más fácil y mejor.

Tener acceso a las tecnologías no es difícil, está abierto a todas las empresas que quieran hacer uso de ellos y desarrollar nuevas capacidades para competir en el mercado laboral para poder manejar equipos tecnológicos ya que estos forman parte de nuestra vida diaria. Las tecnologías deben convertirse en herramientas propulsoras de desarrollo para la seguridad informática, la cual se encuentra en un proceso donde se pretende promover una cultura tecnológica que sea la fuente para crecer en lo social.

El uso de internet ha permitido revolucionar la comunicación y conectividad en redes, pero si bien es claro, también nos vuelve propensos debido a que través de los teléfonos nos conectamos de diferentes dispositivos inalámbricos, fuente que permite el acceso de información personal o la infección de virus a nuestros dispositivos.

En la actualidad el uso de herramientas de seguridad informática puede ayudar a mantener unas bases firmes frente a las vulnerabilidades inmersas en las brechas de seguridad, detectarlas, monitorearlas y hacerles frente a los posibles riesgos.

El objetivo del presente caso de estudio es realizar un análisis comparativo sobre las herramientas de seguridad informática open source Nessus y Snort con el fin de saber cuál de las dos herramientas puede ser aplicado en una empresa. La metodología de investigación que se usó en el presente estudio de caso fue la técnica de investigación

bibliográfica porque recopiló y revisó materiales publicados en internet ya sea libros, revistas, documentos y también de recursos en línea como sitios web, blogs, etc., y como método de investigación se usó la investigación cualitativa donde se analizó la información obtenida de internet. La línea de investigación del presente estudio de caso es Sistemas de información y comunicación, emprendimiento e innovación. La sublínea de investigación Redes y tecnologías inteligentes de software y hardware.

**Desarrollo.**

La Seguridad Informática es un proceso donde se evita y localiza el uso no autorizado de un sistema informático con el objetivo de resguardar la integridad y privacidad de una información que puede estar almacenada en un sistema informático, es decir, busca proteger contra los intrusos el uso de recursos informáticos ya sea con intenciones maliciosas, con intenciones de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente (Netec, s.f.).

Las empresas almacenan información como cuentas bancarias, datos de clientes y proveedores, documentos legales, etc. que son su principal activo y pilar esencial, así, la pérdida, alteración o robo de esta información podría perjudicar seriamente a una empresa ocasionando daños millonarios (Estruga, 2020).

La protección de equipos informáticos es primordial para evitar riesgos que puedan hacer peligrar la estabilidad de una empresa. Es necesario mencionar que la ciberseguridad está directamente ligada la gestión de riesgos empresariales. Invertir en protección informática es una forma de mejorar la rentabilidad y hacer una apuesta en firme para el futuro de una empresa.

Con la finalidad de que una técnica o herramienta de seguridad informática sea efectiva en la protección de datos debe garantizar 4 aspectos:

- **Integridad:** asegurar que la información personal solo puede ser gestionada o eliminada por el usuario y detectar si hubo un acceso no autorizado.
- **Confidencialidad:** proteger el ingreso indebido de terceros a información personal y dinero.

- **Disponibilidad:** garantizar el acceso a su información cuando y desde donde quieras.
- **Autenticación:** asegurar que las personas que forman parte de una comunicación sean realmente ellas y no una identidad suplantada. (Pichincha, 2021)

**Amenazas y vulnerabilidades**

Los peligros de la información están presentes cuando confluyen dos elementos que son: amenazas y vulnerabilidades. Las amenazas pueden venir de cualquier parte, ya sea interna o externa, relacionada con el entorno de las empresas.

Una amenaza es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus trabajos afectando directamente la información o los sistemas que la procesan.

Podemos agrupar las amenazas a la información en cuatro grandes categorías:

- Factores Humanos (accidentales, errores)
- Fallas en los métodos de procesamiento de información
- Desastres naturales
- Actos maliciosos o malintencionados.

Algunas de estas amenazas son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad

- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

**Tipos de seguridad informática**

Cuando hablamos de seguridad informática es importante distinguir entre los distintos tipos de seguridad informática que existen, ya que es muy importante para las empresas ya que todas manejan internet de alguna forma, ya sea para vender sus productos y servicios, ponerse en contacto con el cliente o simplemente para promocionarse. Por lo que deben controlar la seguridad tanto en red como en sus aplicaciones (software) y equipos (hardware) para no recibir ningún ataque o robo de información que sea perjudicial para el porvenir la organización. (VIEWNEXT, 2018)

Los tres tipos de seguridad informática de lo que hablaremos son:

- **Seguridad informática de red:** Se encarga de proteger toda la información que esta accesible a través de internet y que podría ser usada de manera mal intencionada.
- **Seguridad informática de software:** Se encarga de proteger las aplicaciones y el software de amenazas como pueden ser ataques maliciosos, virus, etc.
- **Seguridad informática de hardware:** Se refiere a la protección de computadoras o dispositivos frente a intromisiones o amenazas.

## Herramientas de Seguridad Informática Open Source

En la sociedad de la información que vivimos, es muy importante mantener seguras nuestras redes. Las empresas se esfuerzan en contener y evitar ataques que puedan poner en peligro información confidencial. Para ello, existen una serie de herramientas gratuitas que intentan proteger nuestro sistema de posibles ataques informáticos.

### Nessus

Nessus es una solución de evaluación de vulnerabilidades y configuración de seguridad basada en la nube. Está diseñada para ayudar a los profesionales de la seguridad a identificar y resolver las inseguridades con el fin de proteger a las organizaciones contra los diferentes peligros de seguridad. Incluye plantillas predefinidas que los clientes pueden personalizar con el fin de buscar vulnerabilidades críticas.

### Funciones

Entre las principales funciones de Nessus, se incluyen descubrimiento de activos, escaneo web, administración de políticas, priorización y evaluación de vulnerabilidades. Permite a las empresas adaptar los análisis según las preferencias individuales, lo que asegura el cumplimiento de varios puntos de referencia del Center for Internet Security (CIS) y otras buenas prácticas. Los equipos de seguridad pueden crear informes sobre los tipos de vulnerabilidades; exportarlos en distintos formatos de archivos, como CSV, HTML y XML; ordenar los datos por cliente o equipo; y compartirlos por correo electrónico después de cada análisis para mejorar la transparencia en los procesos.

Nessus incluye un módulo de resultados en vivo que permite a los clientes realizar evaluaciones de vulnerabilidades en modo offline para hallar, validar y priorizar los problemas y así mejorar la seguridad de una empresa. Los equipos también consiguen categorizar las vulnerabilidades similares y presentar los problemas en un solo hilo para agilizar la priorización y garantizar la resolución inmediata de los problemas (GetApp, s.f.)

**Características**

- Genera archivos .nessus que son usados por los productos de tenable como estándar para directivas de análisis y datos de vulnerabilidades.
- Una sesión de directivas, una lista de destinos y los resultados de varios análisis pueden almacenarse todos juntos en un único archivo .nessus que se puede exportar fácilmente.
- La interfaz gráfica de usuario (GUI) muestra los resultados de los análisis en tiempo real, por lo que no deberá esperar que finalice el análisis para ver los resultados.
- Brinda una interfaz unificada para el analizador Nessus el cual es independiente de la plataforma base; es decir, existen las funcionalidades para Windows, Mac OS X y Linux.
- Los análisis seguirán ejecutándose en el servidor, aun si se desconecta por cualquier motivo.
- Los informes de los análisis de Nessus puede encargarse mediante la UI de Nessus y compararse con otros informes. (Valeriano Orozco, 2013)

**Ventajas**

- Nessus puede brindar a los clientes la capacidad de poder identificar las mayores amenazas y responder rápidamente.
- Los paneles de mando de Nessus son más detallados con el fin de ayudar a los clientes a fortalecer las redes contra las amenazas cibernéticas.
- Nessus puede reducir el tiempo y costo de seguridad en la exploración y asegurar a los clientes el cumplimiento de seguridad (SAS, 2020).

**Snort**

Es un sistema de seguridad de red que ayuda a las empresas a monitorear redes, detectar amenazas y administrar respuestas. Está escrito en lenguaje de programación C y fue desarrollado en 1998 por Martin Roesch, actualmente está desarrollado por Cisco. Es un software gratuito de código abierto. También se puede utilizar como rastreador de paquetes para monitorizar el sistema en tiempo real. El administrador de la red puede usarlo para observar todos los paquetes entrantes y encontrar los que son peligrosos para el sistema. Las reglas son bastante fáciles de crear e implementar y se pueden implementar en cualquier tipo de sistema operativo y cualquier tipo de entorno de red. Snort se basa en la captura de paquetes de biblioteca que es una herramienta que se lo puede utilizar ampliamente en analizadores y rastreadores de tráfico de red. Snort puede hallar o encontrar métodos de ataque, incluida la denegación de servicio, el desbordamiento de búfer y los escaneos de puertos sigilosos. (ATICO34, s.f.).

**Funciones**

- Controles o permisos de acceso
- Respuesta a amenazas

- Supervisión de actividades

**Características**

Hay varias características que hacen que Snort sea útil para que las empresas monitoricen sus sistemas y detecten actividades maliciosas. Éstas incluyen (CIBERSEGURIDAD, s.f.):

- **Monitor de tráfico en tiempo real:** Se puede utilizar para monitorizar el tráfico que entra y sale de una red. Monitorizará el tráfico en tiempo real y emitirá alertas a los usuarios cuando descubra paquetes o amenazas potencialmente maliciosos en las redes de Protocolo de Internet (IP).
- **Registro de paquetes:** Habilita el registro de paquetes a través de su modo de registro de paquetes, lo que significa que registra los paquetes en el disco. En este modo, SNORT recopila todos los paquetes y los registra en un directorio jerárquico basado en una dirección IP de una red.
- **Análisis de protocolo:** Puede realizar un análisis de protocolo, que es un proceso de rastreo de red que captura datos en capas de protocolo para análisis adicionales. Esto permite al administrador de la red examinar más a fondo los paquetes de datos potencialmente maliciosos, lo cual es crucial, por ejemplo, en la especificación del protocolo de pila del Protocolo de control de transmisión / IP (TCP / IP).
- **Coincidencia de contenido:** Recopila las reglas por protocolo, como IP y TCP, luego por puertos, y luego por aquellos con contenido y aquellos sin él. Las reglas que tienen contenido utilizan un comparador de patrones múltiples que aumenta el

rendimiento, especialmente cuando se trata de protocolos como el Protocolo de transferencia de hipertexto (HTTP).

- **Huellas digitales del Sistema Operativo:** La toma de huellas dactilares del sistema operativo (SO) utiliza el concepto de que todas las plataformas tienen una pila TCP / IP única. A través de este proceso, SNORT se puede utilizar para determinar el programa del sistema operativo que utiliza un sistema que puede acceder a una red.
- **Instalación en cualquier entorno de red:** SNORT puede implementarse en todos los sistemas operativos, incluso en Linux y Windows, y como parte de todos los entornos de red.
- **Fuente abierta:** Como pieza de software de código abierto, SNORT es gratuito y está disponible para cualquier persona que quiera usar un IDS o IPS para monitorizar y proteger su red.
- **Las reglas son fáciles de implementar:** Las reglas de Snort son fáciles de implementar y permiten que la supervisión y la protección de la red estén en funcionamiento.

**Ventajas.**

- Puede funcionar como sniffer, es decir, como una herramienta donde podemos ver en consola y tiempo real todo el tráfico que ocurre en nuestra red.
- Registro de paquetes que permite guardar en un archivo los registros para su posterior análisis.
- Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se loguea, es decir se puede acceder a la plataforma y así saber cuándo, de dónde y cómo se produjo el ataque (Ortego Delgado, 2017).

**Análisis Comparativo**

A continuación, se realiza un cuadro comparativo entre las herramientas de seguridad informática open source Nessus y Snort

| CARACTERÍSTICAS | NESSUS | SNORT |
|---|---|---|
| Licencia | Gratuito | Gratuito |
| Componentes | No | ➢ Decodificador<br>➢ Preprocesadores<br>➢ Motor de detección<br>➢ Módulos de salida |
| Compatibilidad | Windows y Unix/Linux | Windows y Unix/Linux |
| Reglas | No | Si |
| Funcionalidades | ➢ API<br>➢ Alertas y notificaciones<br>➢ Análisis de vulnerabilidades<br>➢ Controles o permisos de acceso<br>➢ Creación de informes/análisis<br>➢ Escaneo de redes<br>➢ Evaluación de vulnerabilidades | ➢ Controles o permisos de acceso<br>➢ Respuesta a amenazas<br>➢ Supervisión de actividades |

| | | |
|---|---|---|
| | ➢ Gestión de políticas<br>➢ Priorización de vulnerabilidades/amenazas<br>➢ Rastreo de sitios web<br>➢ Respuesta a amenazas<br>➢ Seguridad de aplicaciones web | |
| Captura de paquetes de biblioteca | No | Si |
| Análisis de trafico de red en tiempo real | Si | Si |
| Motor de detección | No | Si |
| Ideal para | Sistema de detección de intrusiones en red (NIDS) de código abierto, gratuito y ligero para Linux y Windows para detectar amenazas emergentes. | Es una solución integral de análisis de vulnerabilidades que proporciona una visibilidad completa de la postura de seguridad de su infraestructura de TI distribuida y compleja. |
| Categorías | ➢ Seguridad<br>➢ Seguridad de aplicaciones web<br>➢ Analizador de vulnerabilidades<br>➢ Herramientas de monitoreo | ➢ Seguridad y privacidad<br>➢ Seguridad cibernética |

*Tabla 1. Cuadro comparativo entre Nessus y Snort*

Autor. María Mosquera


**Análisis comparativo entre Nessus y Snort según Capterra**

*Ilustración 1. Opiniones de usuarios de Nessus*

Fuente. (Capterra, Nessus, s.f.)

*Ilustración 2. Opiniones de usuarios de Snort*

Fuente. (Capterra, Snort, s.f.)

En las ilustraciones 1 y 2 se evaluaron varias características de ambas herramientas de seguridad informática y es posible observar que Nessus es superior en muchos aspectos con respecto a Snort. Algunas de las principales características que Nessus supera a Snort es de forma general, en la facilidad de uso y en las funcionalidades.

## Metodología

### Tipo de investigación

Para el desarrollo del presente estudio de caso se hizo uso del tipo de investigación bibliográfica donde se recopiló y revisó materiales publicados en internet ya sea libros,


revistas, documentos y también de recursos en línea como sitios web, blogs, etc., este tipo de investigación fue uno de los procesos más importante para llevar a cabo la realización de

este proyecto de investigación donde se incluyó la selección de diferentes fuentes de información.

**Técnicas e instrumentos de investigación**

Como se mencionó anteriormente la técnica de investigación que se usó en el desarrollo del estudio de caso fue la investigación bibliográfica donde recopilo información de internet. El instrumento de investigación que se usó fue la investigación cualitativa donde se analizó la información obtenida de internet.

**Conclusiones.**

Una vez finalizado el desarrollo del presente estudio de caso se llegó a las siguientes conclusiones, luego de haber realizado las comparaciones entre las herramientas de seguridad informática open source Nessus y Snort:

- Se registran fallos de seguridad y en muchas ocasiones ocurre por la falta de conocimientos sobre los riesgos que estos acarrean, por lo tanto, los incidentes cada vez más impactan de forma directa a las empresas.
- Es importante que las herramientas de seguridad informática open source sigan contribuyendo con la protección de información en las empresas evitando el uso no

autorizado por parte de personas ajenas a las empresas y así prevenir daños millonarios.

- La herramienta Nessus es usado por muchas empresas ya sea por su funcionalidad, por su análisis de trafico de red en tiempo real, por sus categorías, por su facilidad de manejo, etc.

**Bibliografía.**


ATICO34, G. (s.f.). *Así es Snort, el sistema de detección de intrusos más popular*. Obtenido de GRUPO ATICO34: https://protecciondatos-lopd.com/empresas/snort-deteccion-intrusos/

Capterra. (s.f.). *Nessus*. Obtenido de Capterra: https://www.capterra.ec/software/130577/nessus#reviews

Capterra. (s.f.). *Snort*. Obtenido de Capterra: https://www.capterra.ec/software/1010620/snort#features

CIBERSEGURIDAD. (s.f.). *ANALIZANDO SNORT: SISTEMA DE DETECCIÓN DE INTRUSIONES*. Obtenido de CIBERSEGURIDAD Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas: https://ciberseguridad.com/servicios/sistema-deteccion-intrusos-ids/snort/#Caracteristicas

Derecho, E. d. (28 de Mayo de 2021). *La Seguridad Informática y sus beneficios*. Obtenido de Escuela de Postgrado de Ciencias del Derecho: https://cienciasdelderecho.com/seguridad-informatica-beneficios/

Estruga, N. (28 de Octubre de 2020). *La importancia de la seguridad informática en el entorno empresarial*. Obtenido de EALDE BUSINESS SCHOOL: https://www.ealde.es/importancia-seguridad-informatica-empresas/

GetApp. (s.f.). *Nessus*. Obtenido de GetApp: https://www.getapp.es/software/128439/nessus

Netec. (s.f.). *¿Qué es seguridad informática?* Obtenido de Netec: https://www.netec.com/que-es-seguridad-informatica

Ortego Delgado, D. (9 de Mayo de 2017). *Las 8 mejores herramientas open source de detección de intrusión*. Obtenido de OpenWebinars: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

Ortego Delgado, D. (21 de Marzo de 2017). *Qué es Snort: Primeros pasos*. Obtenido de Open Webinars: https://openwebinars.net/blog/que-es-snort/

Pichincha, B. (10 de Febrero de 2021). *Diez consejos de seguridad informática para tu día a día*. Obtenido de Banco Pichincha: https://www.pichincha.com/portal/blog/post/consejos-seguridad-informatica

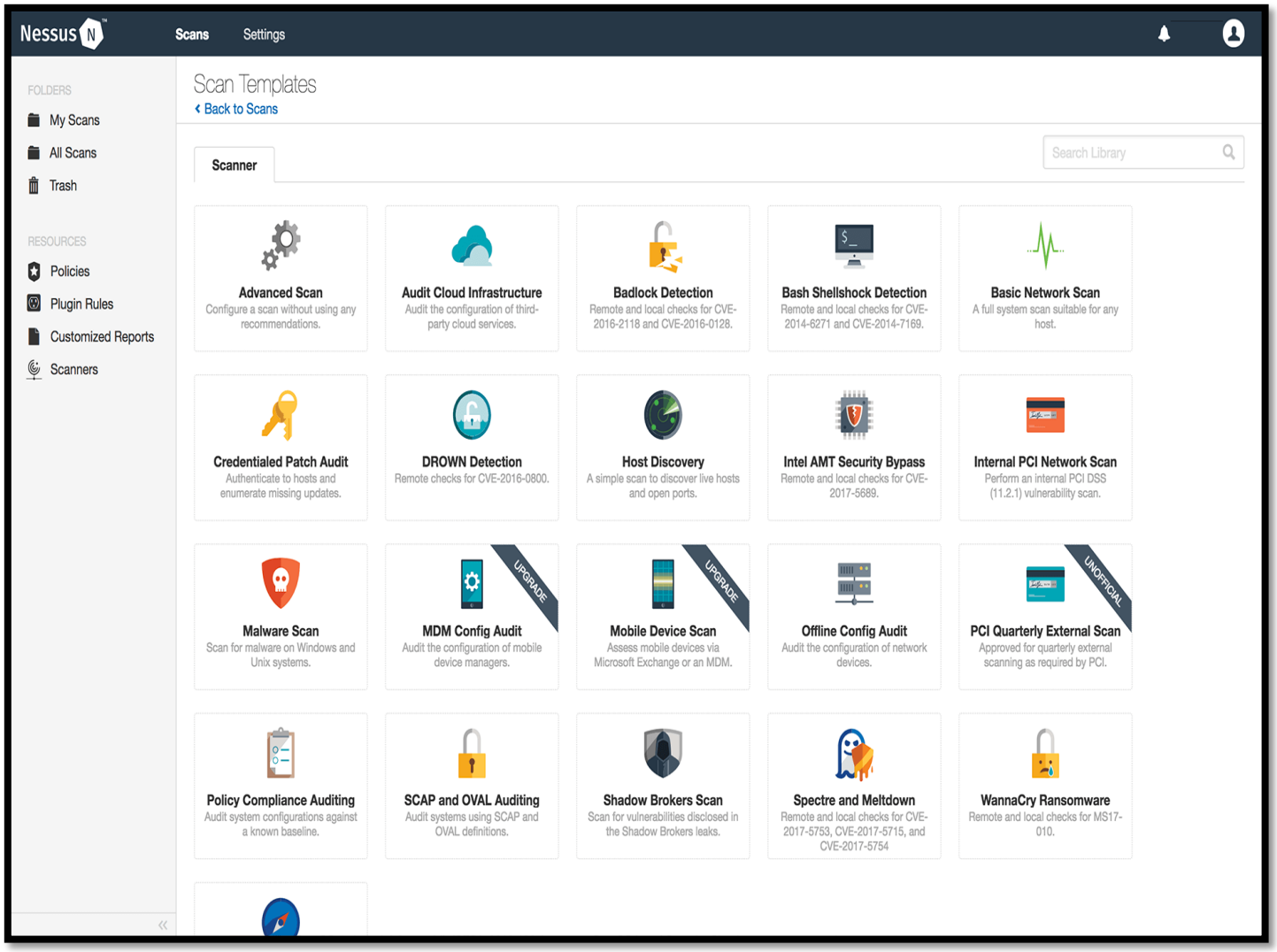
SAS, S. S. (2020). *Nessus*. Obtenido de SEAQ: https://www.seaq.co/nessus.html

Terrell Hanna, K. (Julio de 2021). *Snort*. Obtenido de TECHTARGET NETWORK: https://www.techtarget.com/searchnetworking/definition/Snort

Valeriano Orozco, M. (22 de Octubre de 2013). *3.5 Nessus*. Obtenido de slideshare: https://es.slideshare.net/meztli9/35-nessus

VIEWNEXT. (21 de Febrero de 2018). *Tipos de seguridad informatica*. Obtenido de VIEWNEXT AN IN SUBSIDIARY: https://www.viewnext.com/tipos-de-seguridad-informatica/

VIU. (21 de Marzo de 2018). *Herramientas de seguridad informática más recomendadas en 2018*. Obtenido de Universidad Internacional de Valencia: https://www.universidadviu.com/int/actualidad/nuestros-expertos/herramientas-de-seguridad-informatica-mas-recomendadas-en-2018




**Anexos.**

*Ilustración 3. Plantillas de Escaneo de Nessus*

Fuente. *(Capterra, Nessus, s.f.)*

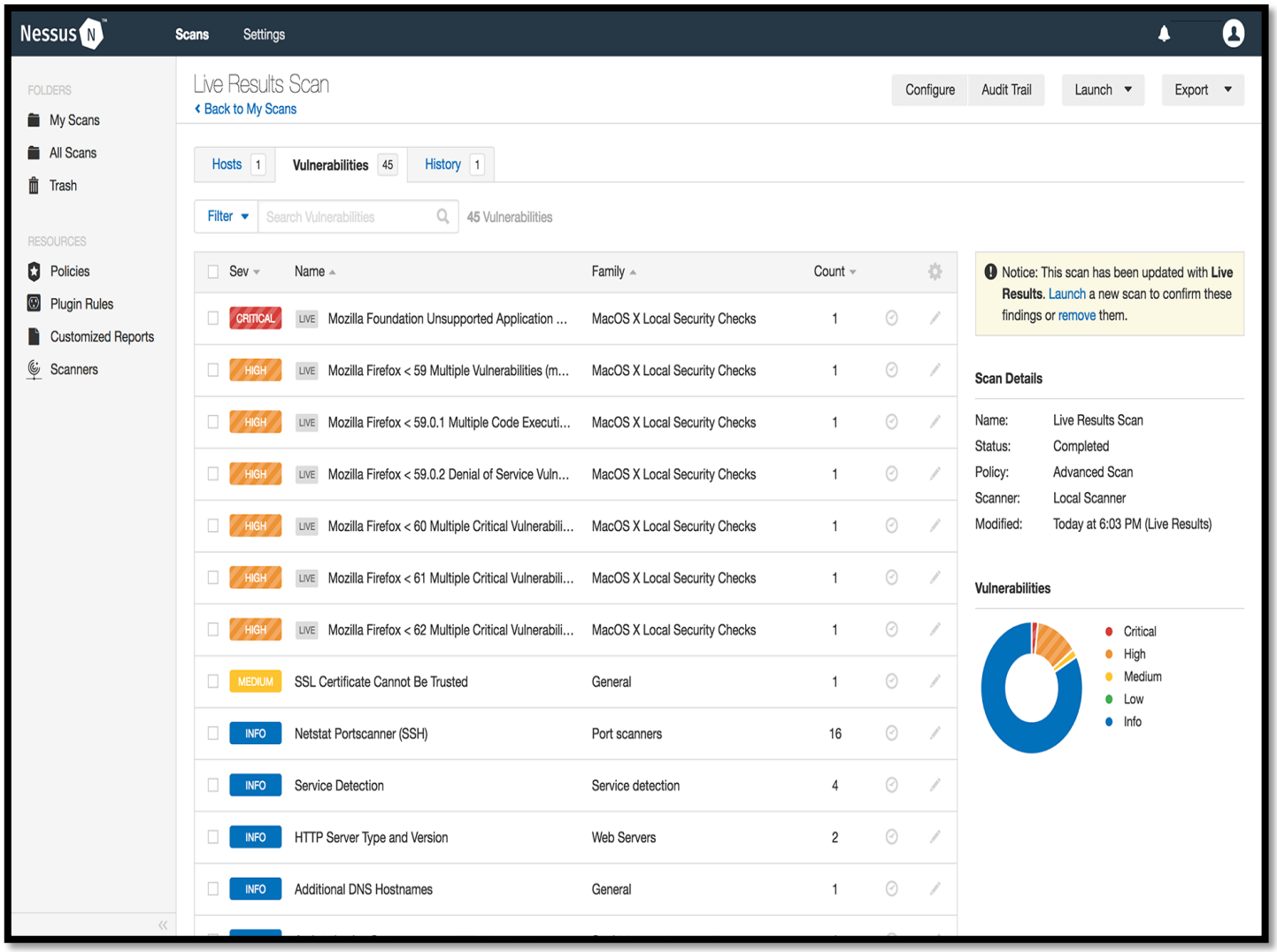



*Ilustración 4. Escaneo de Resultados en tiempo real de Nessus*

Fuente. (Capterra, Nessus, s.f.)

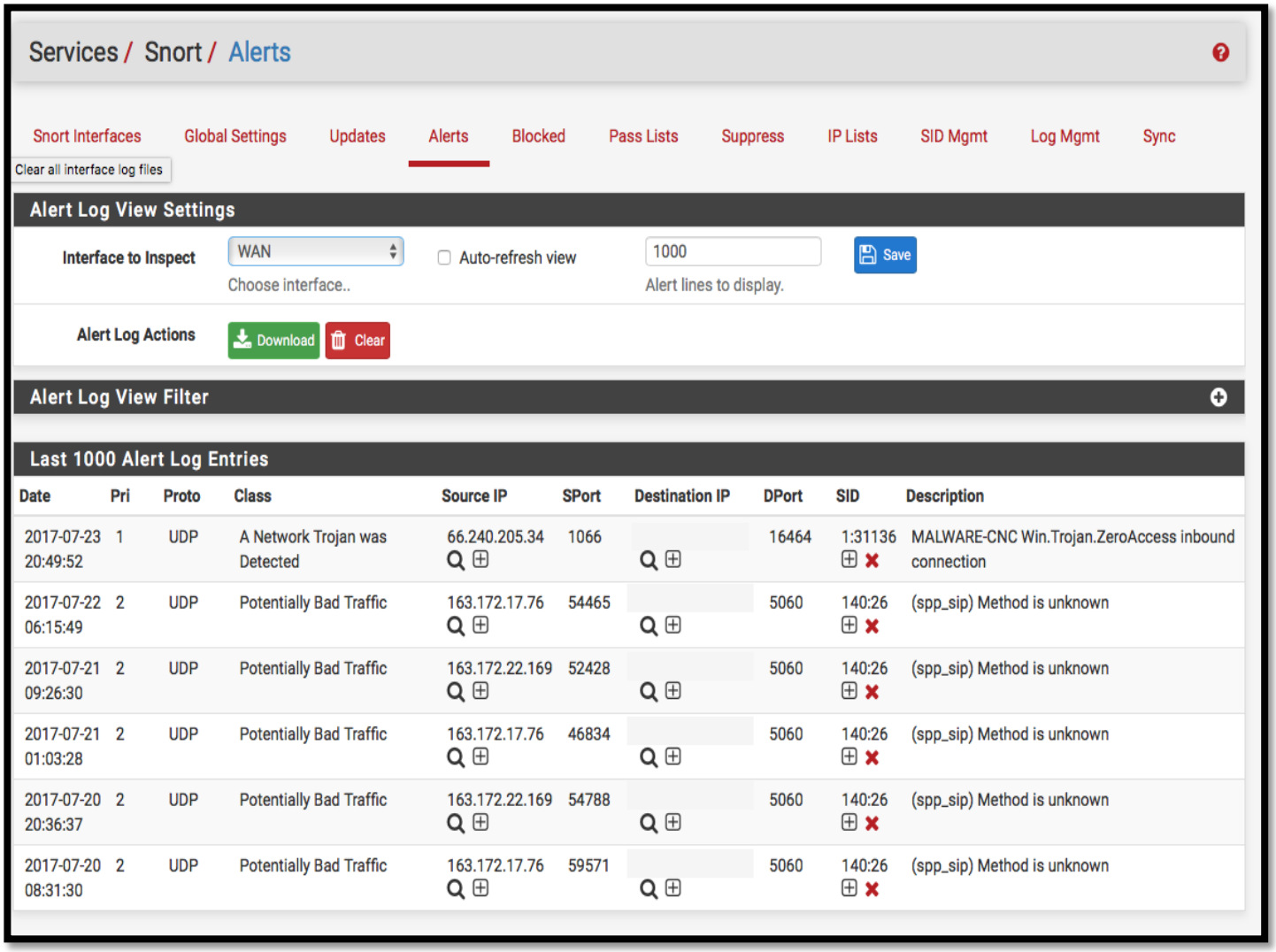



*Ilustración 5. Consola IDS de Snort*

Fuente. (Capterra, Snort, s.f.)

Curiginal

## Document Information

| | |
|---|---|
| **Analyzed document** | Maria_Mosquera_Urkund.docx (D131713322) |
| **Submitted** | 2022-03-27T21:59:00.0000000 |
| **Submitted by** | |
| **Submitter email** | mmosquera776@fafi.utb.edu.ec |
| **Similarity** | 6% |
| **Analysis address** | mzuniga.utb@analysis.urkund.com |

## Sources included in the report

| | | |
|---|---|---|
| SA | **tesis carlos frias.docx**<br>Document tesis carlos frias.docx (D32108234) | 1 |
| W | URL: https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/<br>Fetched: 2020-03-27T11:01:08.8070000 | 2 |
| SA | **TAREA_INVESTIGACION.pdf**<br>Document TAREA_INVESTIGACION.pdf (D120437978) | 1 |
| SA | **CS MSI U2 V1.docx**<br>Document CS MSI U2 V1.docx (D120680832) | 2 |



*Ilustración 6. Reporte Urkund*