



**CONSEJO DE DEFENSA NACIONAL
INSTITUTO DE ALTOS ESTUDIOS ESTRATÉGICOS
PROGRAMA DE ESPECIALIZACIÓN EN
CIBERDEFENSA Y CIBERSEGURIDAD ESTRATÉGICA**



TRABAJO PRÁCTICO GRUPAL

**GRUPO N° 4: “HERRAMIENTAS COMERCIALES
PARA DETECTAR VULNERABILIDADES”**

**Lic. A. Sist. Edgar Wilfrido Ortiz Arza
Ing. Electrónico Jorge Daniel Orué Cuevas
Lic. A. Sist. Diana Liz Jané Otazú
Abogado Federico Manuel Peña Giménez
Lic. Informática Nicolás Pereyra Molinas
Lic. A. Sist. Julio Cesar Planás Montiel
Lic. A. Sist. Gustavo Adolfo Riquelme Medina
Lic. A. Sist. Marcos Darío Rivarola Lebrón
Ana. Sist. Marcos Antonio Riveros Coronel**

**CONSEJO DE DEFENSA NACIONAL
INSTITUTO DE ALTOS ESTUDIOS ESTRATÉGICOS
PROGRAMA DE ESPECIALIZACIÓN EN
CIBERDEFENSA Y CIBERSEGURIDAD ESTRATÉGICA**

TRABAJO PRÁCTICO GRUPAL

**GRUPO N° 4: “HERRAMIENTAS COMERCIALES
PARA DETECTAR VULNERABILIDADES”**

**Lic. A. Sist. Edgar Wilfrido Ortiz Arza
Ing. Electrónico Jorge Daniel Orué Cuevas
Lic. A. Sist. Diana Liz Jané Otazú
Abogado Federico Manuel Peña Giménez
Lic. Informática Nicolás Pereyra Molinas
Lic. A. Sist. Julio Cesar Planás Montiel
Lic. A. Sist. Gustavo Adolfo Riquelme Medina
Lic. A. Sist. Marcos Darío Rivarola Lebrón
Ana. Sist. Marcos Antonio Riveros Coronel**

Asunción, Paraguay

Junio 2019

TABLA DE CONTENIDO

	Página
INTRODUCCIÓN	8
DESARROLLO	10
1. Seguridad de la información.....	10
2. Vulnerabilidades	12
3. Amenazas.....	13
4. Riesgo	13
5. Guías para evaluación de herramientas de vulnerabilidades.	14
6. Recomendaciones generales	15
7. Definición de mercado.....	15
8. Descripción del mercado	16
9. Dirección del mercado	17
10. Análisis de mercado y características nuevas deseadas.....	18
a. Escaneo de aplicaciones web	18
b. Evaluación de configuración de seguridad	19
c. Seguridad en las nubes.....	20
d. Gestión de amenazas y vulnerabilidad.....	21
e. Herramientas BAS	22
f. Pruebas de penetración Pentesting.....	22
g. Vulnerabilidades	23
11. Las mejores herramientas de software para escanear vulnerabilidades	26
a. Nessus	26
b. Alibaba Cloud Vulnerability Discovery Service	27
c. Qualys	27
d. Netsparker	27

e. Amazon Inspector	28
f. AlienVault USM (from AT&T Cybersecurity)	28
g. Intruder.....	29
h. Acunetix Vulnerability Scanner.....	29
i. BurpSuite	29
j. WhiteSource Software	29
12. Comparativo de escáneres de vulnerabilidades según características y puntajes.	30
CONCLUSIÓN	33
BIBLIOGRAFÍA	36

LISTA DE ABREVIATURAS

API	Application Programming Interface
AWS	Amazon Web Services
BAS	Breach and Attack Simulation
BeEF	Browser Exploitation Framework
CSP	Cloud Service Provider
DAST	Dynamic Application Security Testing
DevOps	Development and Operations
ERP	Enterprise Resource Planning
HTML5	HyperText Markup Language, versión 5
IaaS	Infrastructure as a Service
IDPS	Intrusion Detection Prevention System
IoT	Internet of Things
MDR	Managed Detection and Response
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
SaaS	Software as a Service
SAST	Static Application Security Testing
SCA	Security Configuration Assessment
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SPA	Single Page Application
SQL	Structured Query Language
SQLi	SQL Injection
TI	Tecnologías de la Información
USM	Unified Security Management
VM	Virtual Machine
WAF	Web Application Firewall
WTI	Website Threat Inspector
XSS	Cross-Site Scripting

LISTA DE TABLAS

	Página
Tabla 1 Comparativo de características de escáneres de vulnerabilidades	30

LISTA DE FIGURAS

Figuras	Página
Ilustración 1 Riesgo.....	14
Ilustración 2 Puntaje de scaneres de vulnarabilidades	31

INTRODUCCIÓN

En la actualidad, la dinámica de la globalización y evolución constante de las tecnologías, exige a las organizaciones crear nuevas herramientas y métodos de trabajos, diseñar políticas, ejecutar acciones y adecuar sus infraestructuras, a fin de mantener, extender y potenciar sus recursos y habilidades en el sector competitivo que les toca convivir. En este contexto de acción, existe una vinculación activa entre todos los sectores públicos y privados, a nivel nacional e internacional, principalmente a través de la utilización del ciberespacio.

En estas interconexiones entre diferentes actores a través de las telecomunicaciones, no se tienen en cuenta las fronteras físicas de los países, es así que todos los elementos que intervienen, como ser equipos de comunicaciones, aplicaciones informáticas, personas y organizaciones pueden estar interactuando activamente las 24 horas del día con miles de kilómetros de distancias entre sí.

Este entorno global posibilita también la aparición de nuevas amenazas, cada vez más sofisticadas, que pueden poner en riesgo no solamente a las redes y sistemas de información de las organizaciones, sino también afectar a las infraestructuras críticas y a los servicios esenciales de una comunidad, con graves consecuencias para la seguridad nacional. Es necesario, por ende, que las empresas, los activos del estado, las unidades académicas y la ciudadanía en general, tengan opciones para dar una respuesta al desafío presentado.

El desarrollo del presente trabajo de investigación denominado “*Herramientas comerciales para detectar vulnerabilidades*” propone en primer lugar hacer una reseña general de los conceptos básicos de seguridad de la información, así como amenazas y vulnerabilidades a las que se enfrentan las empresas y organizaciones gubernamentales, a la vez realizar un estudio exhaustivo de las principales herramientas con que se cuenta en el mercado comercial utilizadas para este fin.

Se presentan definiciones sobre los conceptos de seguridad de la información y al partir del mismo las ciberamenazas y vulnerabilidades que se pueden presentar sobre la infraestructura con que cuenta la organización. A partir de estas

consideraciones, consensuar sobre la definición de riesgos y las posibilidades e impactos que puedan tener todos estos elementos sobre los activos con que cuentan las diversas entidades.

Posteriormente, se irán analizando aquellas aplicaciones y herramientas informáticas comerciales que tienen mayor impacto en la evaluación de vulnerabilidades.

DESARROLLO

1. Seguridad de la información.

Definimos como seguridad de la información al conjunto de técnicas, medidas preventivas y reactivas¹, políticas y acciones que se llevan a cabo dentro de la organización a fin de resguardar y proteger los datos que se utilizan en la misma.

Se basa en cuatro áreas principales:

Confidencialidad: aspecto que define que la información sea solamente accesible para el personal autorizado. Los datos, recursos e información no deben llegar ni ser utilizados por personas o entidades que no dispongan del permiso requerido para ello.

Integridad: solo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario. Los datos deben estar protegidos frente a vulnerabilidades externas o posibles errores humanos.

Disponibilidad: permite el acceso de los usuarios habilitados, a la información cuando la misma sea requerida teniendo en cuenta su privacidad. Los datos deben ser accedidos en todo momento según los permisos correspondientes.

Autenticación: la información procede del usuario que realmente es quien dice ser.

A la vez implica el proceso de proteger nuestros recursos informáticos contra intrusos que tienen intenciones maliciosas, como para obtener ganancias o imposibilitar el acceso a los mismos, o incluso la posibilidad de acceder a ellos por errores en la arquitectura, omisiones o en forma accidental. Algunas medidas de seguridad implican acciones como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, activación/desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la

¹ Wikipedia. Seguridad de la Información. Consultado 5 de junio 2019. Disponible en https://es.wikipedia.org/wiki/Seguridad_de_la_información

computadora, los recursos de red o de Internet, inclusive medidas como accesos a los recintos protegidos solo para los usuarios permitidos.

Es muy importante la seguridad de la información ya que muchas acciones y/o gestiones realizadas en las organizaciones dependen de las correctas decisiones que se tomen en el ámbito tecnológico. Por ejemplo, prevenir el robo de cuentas bancarias o informaciones de tarjetas de créditos, documentos relacionados al trabajo, denominado muchas veces como espionaje industrial, entre otros. Un ingreso no deseado a sistemas de información puede permitir al intruso modificar o cambiar los códigos fuentes de aplicaciones, utilizar o reemplazar sitios web, crear o inutilizar cuentas de correos que puedan tener contenido perjudicial entre otros.

Existe un grupo de personas denominadas ciberdelincuentes que intentan acceder a las computadoras con intenciones maliciosas como ser atacar a otros equipos o sitios, bloquear equipos y sistemas informáticos para propiciar la pérdida de datos, lanzar ataques de denegación de servicios para impedir la accesibilidad y disponibilidad de servicios o inclusive dañar los mismos.

Todos los factores mencionados indican la necesidad real de que nuestros datos deben permanecer seguros y protegidos en el interior de la organización y solo para los fines que fueron diseñados.

Algunas medidas que pueden ser utilizadas para proteger nuestros activos de información son:

- Instalación y mantenimiento de sistemas antivirus, con reglas de configuración bien definidas.
- Instalación de aplicaciones adquiridas legalmente con las licencias de utilización respectivas.
- Hardware y software que cumplen la función de cortafuegos o firewalls, que ayudan a bloquear y permitir accesos a los entornos de red establecidos.
- Manejo y políticas de contraseñas seguras.

- Conocimiento de ingeniería social para formación y capacitación de los usuarios.
- Encriptación de las informaciones.
- Manejo de políticas de seguridad y buenas prácticas dentro de las organizaciones, entre otros.

2. Vulnerabilidades

Es toda debilidad o fallo en un sistema de información que pueda comprometer o poner en riesgo la integridad, disponibilidad o confidencialidad de los datos en una organización. Pueden tener distintos orígenes como por ejemplos fallos de diseños en equipos o sistemas operativos, errores de configuración en la instalación de aplicaciones, carencias de políticas o procedimientos inadecuados, negligencias por comportamiento del personal, entre otros.

Tipos de vulnerabilidades:

- Baja: impacto mínimo, no afecta a una gran masa de usuarios, muy difícil de aprovechar por el atacante.
- Moderada: el riesgo se presenta se puede disminuir con configuraciones predeterminadas y/o avanzadas, auditorías, entre otras disposiciones.
- Importante: capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de la información y recursos con que cuenta la organización.
- Crítica: permite la propagación de amenazas con un costo muy alto para la organización.

3. Amenazas

Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Puede tener un potencial muy negativo sobre nuestros datos. Las amenazas pueden proceder de ataques que pueden producir fraudes, robos de datos, instalación de malware o virus informáticos, entre otros. También pueden provenir de sucesos físicos como ser incendios, inundaciones, tormentas, rayos, entre otros factores climáticos, o inclusive desde el sector interno de la organización atribuido a negligencias y malas políticas institucionales como ser mal manejo de contraseñas, no utilización de transmisiones y/o aplicaciones cifradas, etc.

Una amenaza existe a partir de la existencia de vulnerabilidades que puedan ser aprovechadas y pueden clasificarse en amenazas intencionales, que deliberadamente intenta causar un daño (como por ej. El robo de información utilizando técnicas de ingeniería social), o no intencionales, donde a causa de acciones u omisiones se ponen en riesgo los activos de información y pueden producir un daño.

4. Riesgo

El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo la existencia de vulnerabilidades frente a una determinada amenaza, cómo lo sería un ataque de denegación de servicios o de un virus. El riesgo depende entonces de que la amenaza aproveche una vulnerabilidad y produzca un impacto.



Ilustración 1 Riesgo

5. Guías para evaluación de herramientas de vulnerabilidades.

El mercado tecnológico actual, en herramientas comerciales utilizadas para gestión de las vulnerabilidades, se encuentra en una etapa de madurez y robustez, las grandes corporaciones de todos los sectores, financieros, de producción, académicos y las principales instituciones gubernamentales de muchos países utilizan en forma cotidiana estas aplicaciones informáticas, algunas indiscutiblemente son líderes en su sector.

Sin embargo, el gran desafío se presenta a partir de la irrupción de tecnologías emergentes que abren un nuevo espacio de oportunidades para las amenazas, como, por ejemplo:

- Aplicaciones, motores de bases de datos, servicios, que se ejecutan en plataformas ubicadas en la nube, se están desarrollando a un ritmo vertiginoso.
- La tecnología de los dispositivos móviles y las aplicaciones que se ejecutan sobre las mismas.

- Interconexión digital de objetos cotidianos con internet, IoT o internet de las cosas.

6. Recomendaciones generales

Los encargados de la seguridad de la información y gestión de riesgos en las organizaciones deben evaluar estas características:

- El flujo de trabajo, la gestión empresarial y las integraciones de tecnología de terceros que las herramientas comerciales proporcionan como anexos a su aplicación principal. Estos incluyen sistemas de prevención de intrusos y firewalls de aplicaciones web, así como herramientas de priorización de riesgos, como la gestión de amenazas y vulnerabilidades y herramientas de simulación de violaciones, para respaldar más efectivamente las operaciones de seguridad.
- Seleccionar las herramientas de vulnerabilidades teniendo en cuenta la cobertura de tecnologías y enfoques emergentes, como ser aplicaciones en la nube y la virtualización, DevOps, contenedores de software. Se puede requerir más de un proveedor si se tienen estas tecnologías en la organización.
- Analizar las metodologías que utiliza la herramienta para la evaluación del impacto, criticidad y priorización de vulnerabilidades, para que puedan ser administradas de manera más eficiente en la organización.

7. Definición de mercado

El mercado de herramientas comerciales para evaluación de vulnerabilidades está formado por proveedores que brindan capacidades para identificar, categorizar y gestionar vulnerabilidades. Estos incluyen configuraciones no seguras del sistema, configuraciones predeterminadas o actualizaciones faltantes, así como otras actualizaciones relacionadas con la seguridad en los sistemas conectados a la red local directamente, de forma remota o en la nube. Los productos o servicios de estas herramientas tienen varias capacidades comunes:

- Descubrimiento e identificación de activos de TI conectados a la red.
- Posibilidad para identificar y rastrear cambios en el estado de las bases de datos en múltiples períodos de tiempo (días, semanas, meses, etc.)
- Informes o reportes con formato preestablecidos de cumplimiento de estándares específicos.
- Soporte para la evaluación pragmática de riesgos con capacidad de evaluar la gravedad de la vulnerabilidad, la criticidad de los activos y el uso prevaleciente por parte de los atacantes, utilizando inteligencia de amenazas y varios algoritmos de análisis y aprendizaje automático
- La capacidad de comprender cómo un atacante puede actuar en un entorno y qué sistemas/técnicas serán exitosos.
- Soporte con información, orientación de priorización y recomendaciones para remediar y configurar controles alternativos.
- La capacidad de conectarse a otras herramientas de gestión y tratamiento de tickets para descubrir, actuar y confirmar la resolución de vulnerabilidades.

8. Descripción del mercado

Existen herramientas comerciales de vulnerabilidades que se instalan como una solución local basada en software o dispositivos, también pueden ejecutarse desde la nube, o tener un híbrido de estas opciones.

Las herramientas que permiten realizar simulaciones de ataque y ataque (BAS) representan un mercado nuevo y emergente. Realizan pruebas automatizadas de seguridad y modelado de cadenas de ataque que identifican la ruta más probable que un atacante usaría para comprometer un ambiente. La mayoría de las veces, esto se basa principalmente en aprovechar el conocimiento de las vulnerabilidades en términos de identificación e intento de explotación. También ayudan a presentar una

visión más real de las vulnerabilidades que conducirán a una violación frente a la cantidad total de vulnerabilidades presentes.

Estas simulaciones utilizan casos de usos estándares como por ejemplo los relaciones al ámbito del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) o el Instituto Nacional de Estándares y Tecnología (NIST).

El mercado se caracteriza por proveedores de seguridad más pequeños o medianos en comparación con los proveedores de seguridad y antimalware de redes más grandes. Algunos son de propiedad privada, por lo general ofrecen ofertas principalmente en torno a las herramientas comerciales y en cambio algunos proveedores más grandes incluyen a la gestión de vulnerabilidades como un componente de una cartera de tecnologías o servicios de administración de seguridad unificada más amplia, como por ejemplo McAfee, IBM y Symantec.

9. Dirección del mercado

El mercado de herramientas comerciales de vulnerabilidades está maduro y el crecimiento general del mercado es estable. Estas herramientas constituyen un estándar de la mayoría de los marcos regulatorios y de gestión de la seguridad de la información. Los ingresos en el mercado se concentran entre unos pocos proveedores, y un gran porcentaje va a tres proveedores (Rapid7, Tenable y Qualys). Además de competir con otros proveedores de productos y servicios, también deben competir con consultores, herramientas de escaneo de código abierto y otros productos de seguridad y operaciones de TI que brindan capacidades de evaluación de escaneo y configuración. Muchos proveedores tienen versiones más básicas de sus productos disponibles de forma gratuita, que muchas empresas medianas usan para escanear sus instalaciones.

Estas herramientas se encuentran en plataformas comunes, como Windows o Linux, con solo pequeñas diferencias entre las soluciones en términos de alcance y cobertura. La competencia cada vez está más basada en precios, en lugar de características.

Una serie de nuevos métodos de entrega de TI funcionan de maneras fundamentalmente diferentes, como la nube en general, DevOps y la computación sin servidor, y plantean desafíos desde un punto de vista de estas herramientas de vulnerabilidades que no permiten la reutilización de los enfoques existentes. Como resultado, el soporte para estas nuevas tecnologías es inmaduro y rara vez puede ser totalmente cubierto por una sola solución informática.

Al mismo tiempo, muchos proveedores también están expandiendo sus carteras con productos en dominios adyacentes, como administración de registros, detección y respuesta administrada (MDR), análisis de seguridad, pruebas dinámicas de seguridad de aplicaciones, evaluación de contenedores y evaluación de servicios en la nube.

10. Análisis de mercado y características nuevas deseadas.

a. Escaneo de aplicaciones web

Esta capacidad de evaluación ahora es ofrecida por todos los principales proveedores de alguna forma. Las herramientas DAST dedicadas siguen ofreciendo una mayor eficacia, especialmente cuando se trata de aplicaciones desarrolladas a medida que las soluciones comerciales que realizan el escaneo general de aplicaciones web. Estas soluciones a menudo vienen con pruebas de seguridad de aplicaciones de software (SAST, por sus siglas en inglés), que complementan a DAST al respaldar la auditoría de código fuente.

En resumen, lo que separa a las herramientas comerciales de vulnerabilidades de las herramientas de DAST es la capacidad de las herramientas de DAST para descubrir nuevas vulnerabilidades en software comercial de tipos seleccionados (principalmente en la web) y, en particular, encontrar vulnerabilidades en aplicaciones desarrolladas a medida. Sin embargo, estas herramientas no pueden descubrir vulnerabilidades en el nivel de lógica de negocios, ni pueden encontrar tipos de vulnerabilidades de código completamente desconocidos. Las herramientas DAST son comúnmente ejecutadas por equipos de seguridad de aplicaciones, en lugar de equipos de operaciones de seguridad. Idealmente, esto debería suceder como

parte de un ciclo de vida de desarrollo de software (SDLC), que se utiliza para desarrollar software. Esto debería ocurrir antes de que una aplicación se ponga en producción o como componente de un SDLC.

Para este propósito, existe una gama de herramientas de código abierto y comerciales que también son populares entre los profesionales como los analizadores de penetración. Los equipos internos y consultores que brindan seguridad web están utilizando herramientas como Burp Suite, w3af, Nikto, WebScarab y The Browser Exploitation Framework (BeEF).

Vendedores representativos: Fortify
IBM AppScan
Qualys
Acunetix
Rapid7
Tenable

b. Evaluación de configuración de seguridad

SCA Security Configuration Assessment: Ofrece la capacidad de evaluar y verificar de forma remota la configuración, como la complejidad de las contraseñas en las políticas de grupo de dominios de Windows. Todos los proveedores encuestados ofrecen esta capacidad de alguna forma, aunque algunos pueden requerir una licencia por separado. Con frecuencia se usa para cumplir con el cumplimiento de las normativas, como PCI, o el cumplimiento de la política de seguridad interna. Esta integración abarca desde comprobaciones de políticas de contraseña básicas hasta análisis de control avanzado a nivel de aplicación.

Mejores herramientas:	Amazon
	Tenable
	Rapid7
	BeyondTrust
	Tripwire
	IBM Bigfix
	Tanium
	Qualys

c. Seguridad en las nubes

La mayoría de los profesionales de la seguridad ahora están acostumbrados a ejecutar herramientas de evaluación tradicionales contra máquinas virtuales (VM) que se ejecutan en las nubes como Amazon Web Services (AWS), Microsoft Azure y Google Cloud. Esta es, por supuesto, una buena práctica, ya que la infraestructura pública como un servicio (IaaS) no le evitará tener que parchear y mantener las cargas de trabajo que se ejecutan allí.

Sin embargo, la parte que falta en la administración de vulnerabilidades en la nube pública implica evaluar el "panel de control" de su servidor en la nube pública. La gran cantidad de organizaciones que tienen elementos como los cubos de Amazon S3 abiertos al mundo es un buen ejemplo de este problema. Los líderes de seguridad de TI deben abordar con urgencia esta brecha de seguridad. Se puede acceder a este panel de control desde cualquier lugar en Internet y, literalmente, se controla su "centro de datos virtual / computación en la nube".

Esto es similar a hacer una evaluación de vulnerabilidad tradicional con el importante matiz del uso de las API del CSP para evaluar la configuración del plano de administración / control de su servidor en el (los) servicio (s) en la nube. Esto se aplica no solo a IaaS, sino también a SaaS y PaaS. Las API admiten la capacidad rápida y programática de instrumentar la nube, lo que las hace ideales para funciones de evaluación. La API también se puede utilizar para solucionar problemas en tiempo casi real; no son solo pasivos. Los líderes de seguridad deben prestar atención a cómo se pueden aplicar estas API a los casos de uso de seguridad, y aprovecharlas

para evaluar cómo ha configurado sus instancias de la nube y utilizarlas para notificarle casi en tiempo real los cambios en su postura y permitir la remediación.

En la mayoría de los casos, aún se requieren ofertas y soluciones especializadas de terceros, más allá de algunas ofertas de servicios generales. Los CSPs líderes, como Amazon y Microsoft, ofrecen algunas de estas funciones, pero generalmente son para sus propias soluciones y no cubren otros servicios en la nube. Los ejemplos incluyen Amazon Inspector y Microsoft Security Center para Azure.

Vendedores representativos:

- Amazon
- Alert Logic
- CloudChecker
- Cavirin
- Dome9
- Evident.io (Palo Alto Networks)
- Microsoft
- RedLock
- Saviynt
- Tenable
- Qualys

d. Gestión de amenazas y vulnerabilidad

Estas herramientas admiten telemetría de vulnerabilidad, las pruebas dinámicas de aplicaciones web y los datos de pruebas de penetración.

Su principal beneficio es lo que hacen con la telemetría. Utilizan diversas formas como la inteligencia de amenazas sobre la actividad de los atacantes y el uso de vulnerabilidades en programas maliciosos, criticidad de los activos internos, para proporcionar una visión fundamental del riesgo real de una organización y entender el riesgo cibernético y ayudar a prevenir una violación de seguridad.

El beneficio es que a los equipos de seguridad se les presenta una lista generalmente más pequeña de problemas de alto riesgo. Estos pueden luego asignarse directamente a las herramientas que los equipos de seguridad ya han

implementado y han administrado durante más de una década, como los sistemas de detección/prevencción de intrusos (IDPS) y/o los sistemas de firewall de aplicaciones web (WAF), para ayudar con la configuración.

Vendedores representativos: Kenna Security
 NopSec
 RiskSense
 Skybox Security
 Core Security
 Risk Based Security

e. Herramientas BAS

Los proveedores de BAS han estado surgiendo en los últimos años y cuentan con tecnología que se implementa en varias partes de la red (que a menudo utilizan agentes) para probar activamente su entorno en busca de problemas, simulando métodos comunes utilizados por los atacantes. Los encargados de seguridad pueden usar esto para priorizar qué acciones tomar a continuación, desde la configuración de los controles de compensación (sistema de prevención y detección de intrusiones (IDPS), WAF, etc.) hasta la segmentación de la red y la aplicación de parches.

Vendedores representativos: AttackIQ
 Cymulate
 Core Security
 Threatcare
 Verodin
 Picus
 Safe Breach
 XM Cyber
 PCYSYS

f. Pruebas de penetración Pentesting

La industria de pruebas ya está bien establecida y muy disputada por proveedores extremadamente grandes, como:

- IBM
(<https://www.ibm.com/security/services/penetration-testing>),
- Accenture
(<https://www.accenture.com/au-en/service-cyber-defensesolutions>)
- Deloitte
(<https://www2.deloitte.com/hu/en/pages/risk/solutions/cyber-risk-vulnerability.html>)

Así como pequeños proveedores como:

- Assurance.com.au
(<http://www.assurance.com.au/>),
- Sense of Security
(<https://www.senseofsecurity.com.au/consulting/penetration-testing>)
- Insomnia Security
(<https://www.insomniasec.com/>).

No existe una correlación entre el tamaño de la organización y la calidad de su trabajo. Las empresas pequeñas continúan siendo muy competitivas

En el contexto de esta investigación específica, las pruebas de penetración desempeñan un papel importante en la "priorización" y la evaluación de vulnerabilidades. Estos servicios están probando su entorno, con habilidades y conocimientos del mundo real del panorama de amenazas prevaleciente. Los encargados de seguridad deben tomar estas aplicaciones y usarla directamente en los programas de riesgo y seguridad.

Además, algunas herramientas de TVM, como Kenna Security y NopSec , pueden procesar datos de estos informes que provienen de pruebas de penetración .

g. Vulnerabilidades

Se aplican métodos que analizan y priorizan las vulnerabilidades mediante el uso de la inteligencia de amenazas, el contexto organizativo y los enfoques de modelos de riesgo, como el análisis de la ruta de ataque. Esta es también un área en

la que también se utilizan métodos analíticos avanzados, como el aprendizaje automático. Las clasificaciones de riesgo se proporcionan a cada vulnerabilidad en función de un motor de procesamiento de datos de evaluación patentado.

Vendedores representativos: Kenna Security
Nopsec
Skybox Security
RiskSense

Los proveedores que proporcionan capacidades avanzadas de dispositivos comunes basados en red, así como características para permitir el análisis, la generación de informes y la gestión de vulnerabilidades y remediación.

<u>Vendedores de TVM</u>	Kenna Security
	NopSec
	RiskSense
	RedSeal
	Skybox
	Core Security
	Risk Based Security
	Qualys
<u>Vendedores de BAS</u>	Safe Breach
	Cymulate
	Threatcare

<u>Vendedores de herramientas</u>	AlienVault
<u>de vulnerabilidades</u>	AlertLogic
	Beyond Trust
	Beyond Security
	Core Security
	CrowdSike
	Digital Defense
	F-Secure
	Greenbone networks
	Outpost24
	Positive Technologies
	Qualys
	Rapid7
	Tenable
	Tripwire

Los encargados de la seguridad y gestión de riesgos deben:

- Evaluar la cobertura de aplicaciones y sistemas operativos de terceros, especialmente para aquellos que se implementan y que no se consideran de uso general

Aunque obtener una cobertura del 100% es lo ideal, desde un punto de vista práctico, cubrir el mayor número posible de tecnologías es un resultado pragmático aceptable. Las evaluaciones en profundidad de las bases de datos y las aplicaciones, como los sistemas ERP (por ejemplo, SAP u Oracle), no son ampliamente compatibles con las soluciones tradicionales, que generalmente se centran en dispositivos, sistemas operativos y configuraciones.

11. Las mejores herramientas de software para escanear vulnerabilidades²

Los escáneres de vulnerabilidad son herramientas que monitorean constantemente las aplicaciones y redes para identificar vulnerabilidades de seguridad. Funcionan manteniendo una base de datos actualizada de vulnerabilidades conocidas y realizan análisis para identificar posibles exploits.

Los escáneres de vulnerabilidad son utilizados por las compañías para probar aplicaciones y redes contra vulnerabilidades conocidas e identificar nuevas vulnerabilidades.

Los escáneres suelen producir informes analíticos que detallan el estado de una aplicación o la seguridad de la red y proporcionan recomendaciones para solucionar problemas conocidos. Algunos escáneres de vulnerabilidad funcionan de manera similar a las herramientas de prueba de seguridad de aplicaciones dinámicas (DAST), pero las herramientas de escaneo en lugar de simular ataques o realizar pruebas de penetración.

Para incluir en la categoría de Escáner de vulnerabilidad, un producto debe:

- Mantener una base de datos de vulnerabilidades conocidas.
- Escanear continuamente las aplicaciones en busca de vulnerabilidades
- Producir informes analizando vulnerabilidades conocidas y nuevos exploits.

a. Nessus

Diseñado por y para profesionales de la seguridad, Nessus Professional es el estándar de facto de la industria para la evaluación de vulnerabilidades. Realiza evaluaciones puntuales para ayudar a los profesionales de seguridad a identificar y corregir vulnerabilidades con rapidez y facilidad, incluidos fallas de software, parches faltantes, malware y configuraciones erróneas, en una variedad de sistemas

² G2. Best Vulnerability Scanner Software. Consultado 5 de junio 2019. Disponible en <https://www.g2.com/categories/vulnerability-scanner>

operativos, dispositivos y aplicaciones. Está diseñado para hacer que la evaluación de vulnerabilidades sea simple, fácil e intuitiva, con características tales como políticas y plantillas creadas previamente, informes personalizables, funcionalidad de "repetición" en grupo y actualizaciones en tiempo real. El resultado: menos tiempo y esfuerzo para evaluar, priorizar y remediar problemas.

b. Alibaba Cloud Vulnerability Discovery Service

Website Threat Inspector (WTI) utiliza datos, pruebas de penetración y aprendizaje automático para proporcionar una solución de seguridad todo en uno para dominios y otros activos en línea. Detecta vulnerabilidades web, contenido ilícito, desfiguración de la página web y puertas traseras que puedan causar posibles pérdidas financieras por mala reputación.

c. Qualys

El enfoque integrado de Qualys para la seguridad y el cumplimiento de TI permite a las organizaciones de todos los tamaños lograr con éxito iniciativas de gestión de vulnerabilidades y cumplimiento de políticas de manera conjunta.

Qualys Cloud Suite incorpora las siguientes aplicaciones, todas a través de la nube: AssetView, Gestión de vulnerabilidades; Monitoreo continuo; ThreatPROTECT; Cumplimiento de políticas; Cuestionario de evaluación de seguridad; Cumplimiento de PCI; Escaneo de aplicaciones web; Firewall de aplicaciones web; Detección de malware.

d. Netsparker

Netsparker desarrolla una solución de seguridad de aplicaciones web automatizada líder en la industria. Disponible como software de Windows, en línea y en servicio local, el escáner Netsparker puede detectar automáticamente Inyección de SQL, secuencias de comandos entre sitios y otras vulnerabilidades en cualquier tipo de HTML5 moderno, aplicación de página única (SPA), aplicación web y servicios web Web 2.0, independientemente de la tecnología con la que están contruidos. El escáner Netsparker no solo informa las vulnerabilidades, sino que también genera

una prueba de vulnerabilidad que confirma que son reales y no falsos positivos. Por lo tanto, no tiene que perder tiempo en verificar manualmente los hallazgos del escáner y puede ampliar fácilmente la seguridad de las aplicaciones web y escanear miles de sitios web en cuestión de horas.

e. Amazon Inspector

Amazon Inspector es un servicio de evaluación de seguridad automatizado que ayuda a mejorar la seguridad y el cumplimiento de las aplicaciones implementadas en AWS. Evalúa automáticamente las aplicaciones en busca de vulnerabilidades o desviaciones de las mejores prácticas.

f. AlienVault USM (from AT&T Cybersecurity)

AlienVault USM Anywhere es una solución de administración de seguridad basada en la nube que acelera y centraliza la detección de amenazas, la respuesta a incidentes y la administración de cumplimiento para la nube, nube híbrida y entornos locales. USM Anywhere incluye sensores en la nube diseñados específicamente para monitorear de forma nativa sus servicios web de Amazon (AWS) y los entornos de nube de Microsoft Azure. En las instalaciones, los sensores virtuales se ejecutan en Microsoft Hyper-V y VMware ESXi para monitorear una nube privada virtual y la infraestructura física de TI. Se puede implementar rápidamente sensores en la nube y en entornos locales mientras administra de forma centralizada la recopilación de datos, el análisis de seguridad y la detección de amenazas.

Cinco capacidades de seguridad esenciales en una sola plataforma SaaS, que le brinda todo lo que necesita para la detección de amenazas, respuesta a incidentes y gestión de cumplimiento, todo en un solo panel. Puede escalar fácilmente para satisfacer sus necesidades de detección de amenazas a medida que su entorno de nube híbrida cambia y crece. 1. Detección de activos; 2. Evaluación de vulnerabilidad; 3. Detección de intrusiones; 4. Monitoreo del comportamiento; 5. SIEM

g. Intruder

Un escáner de vulnerabilidad proactivo, para infraestructura externa. Basado en la nube, encuentra debilidades de seguridad cibernética en los sistemas más expuestos, para evitar costosas violaciones de datos.

h. Acunetix Vulnerability Scanner

Acunetix es líder en el mercado de la tecnología de pruebas de seguridad web automática que escanea y audita con precisión todas las aplicaciones web, incluidas las aplicaciones HTML5, JavaScript y de página única (SPA). Ofrece una entrada rentable en el mercado de escaneo web con una solución simple, escalable y de alta disponibilidad, sin comprometer la calidad. Puede informar sobre una amplia gama de vulnerabilidades web, incluidas SQLi y XSS, y proporciona la única tecnología en el mercado que puede detectar automáticamente vulnerabilidades fuera de banda. También incluye funciones de gestión de vulnerabilidades integradas para que las empresas gestionen, prioricen y controlen de forma integral las amenazas de vulnerabilidades, ordenadas por la criticidad del negocio. Utilizado por muchos sectores gubernamentales, militares, educativos, de telecomunicaciones, bancarios, financieros y de comercio electrónico, está disponible en Windows, Linux y en línea

i. BurpSuite

Burp Suite es un conjunto de herramientas para pruebas de seguridad de aplicaciones web.





j. WhiteSource Software

WhiteSource ayuda a las empresas a desarrollar un mejor software aprovechando el poder del código abierto. WhiteSource pasa a formar parte del ciclo de vida de desarrollo de software (SDLC) y automatiza todo el proceso de selección, aprobación y administración de componentes de código abierto, incluida la búsqueda y reparación de componentes vulnerables. Ofrece a los equipos de seguridad y desarrollo de software control total y visibilidad sobre su uso de código abierto y ayuda a impulsar la adopción de código abierto.

12. Comparativo de escáneres de vulnerabilidades según características y puntajes.

Tabla 1 Comparativo de características de escáneres de vulnerabilidades

Cuadro Comparativo de Análisis de Vulnerabilidades			
	Analizadores	Características Principales	Puntaje (Total 5)
1	Nessus 	Interfaz Unificada Análisis Inteligente Arquitectura modular Arquitectura de plugins BD muy completa y actualizada de vulnerabilidades	4.4
2	Alibaba Cloud Vulnerability Discovery Service 	Software como servicio Detección integral de activos relacionados. Exploración profunda y profesional de vulnerabilidades. Detecta contenidos (pornografía, terrorismo, violencia, etc) Detecta manipulaciones y drive-by-download Reportes gráficos Incluye verificación de riesgos y resoluciones	4.8
3	Qualys 	Software como servicio Gestión completa de vulnerabilidades Monitoreo continuo Reportes completos y personalizables Generación y control de Políticas	4.3
4	Netsparker 	Identificación y reportes para falsos positivos Altamente diseñado para vulnerabilidades de Inyección SQL Generación de reportes en varios formatos Software como servicio	4.4
5	Amazon Inspector 	Motor de análisis de la configuración y monitorización de actividad Biblioteca de contenidos integrada Automatización mediante API Software como servicio	4.2
6	Nexpose 	Soporta Múltiples plataformas Versión móvil Interfaz amigable BD de vulnerabilidades muy completa	4.3

Cuadro Comparativo de Análisis de Vulnerabilidades			
	Analizadores	Características Principales	Puntaje (Total 5)
7	AlienVault USM (from AT&T Cybersecurity) 	Precio Bajo	4.5
		Soporte rápido y efectivo	
		Escaneo rápido y completo en tiempo real	
		Fácil de usar	
8	Intruder 	Automatización de Procesos	4.9
		Auditoría cuando se descubre una nueva vulnerabilidad	
		Análisis de vulnerabilidades muy completo	
9	Acunetix Vulnerability Scanner 	Test avanzado y análisis profundo	4.1
		Especializado para aplicaciones Web	
		Análisis de Vulnerabilidades ultra rápido	
		Multitarea	
10	BurpSuite 	Escáner de vulnerabilidad web muy completo	4.7
		Escaneo programado y automático	
		Escalabilidad ilimitada (multitarea)	
		Integración continua con desarrollo de aplicaciones	

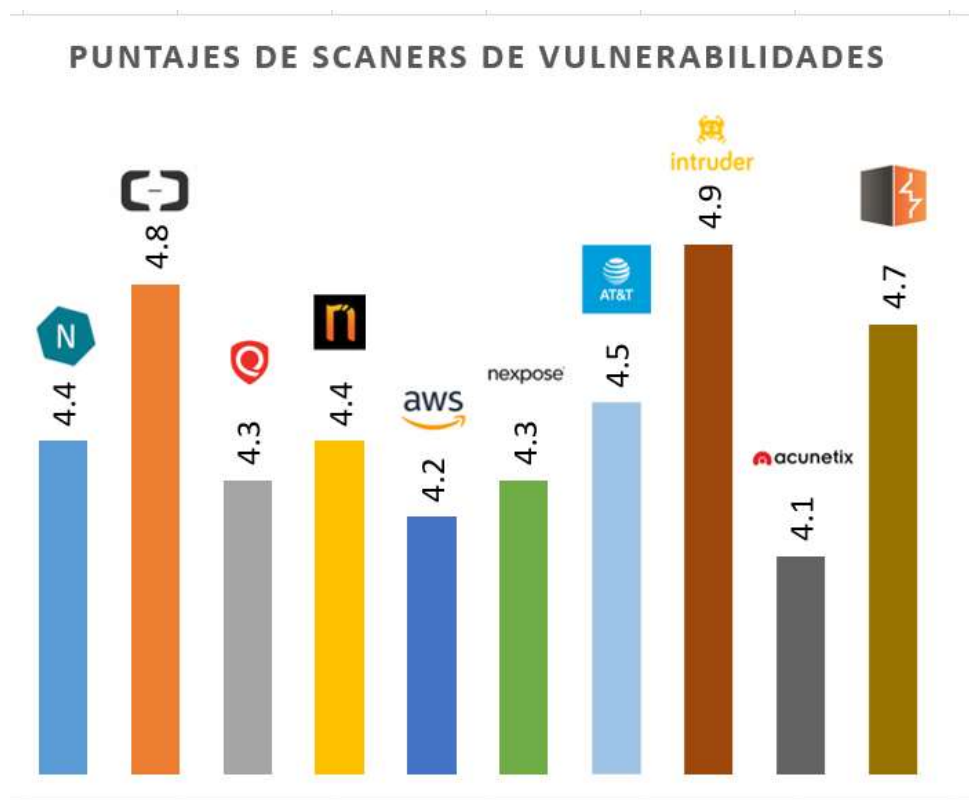


Ilustración 2 Puntaje de escáneres de vulnerabilidades

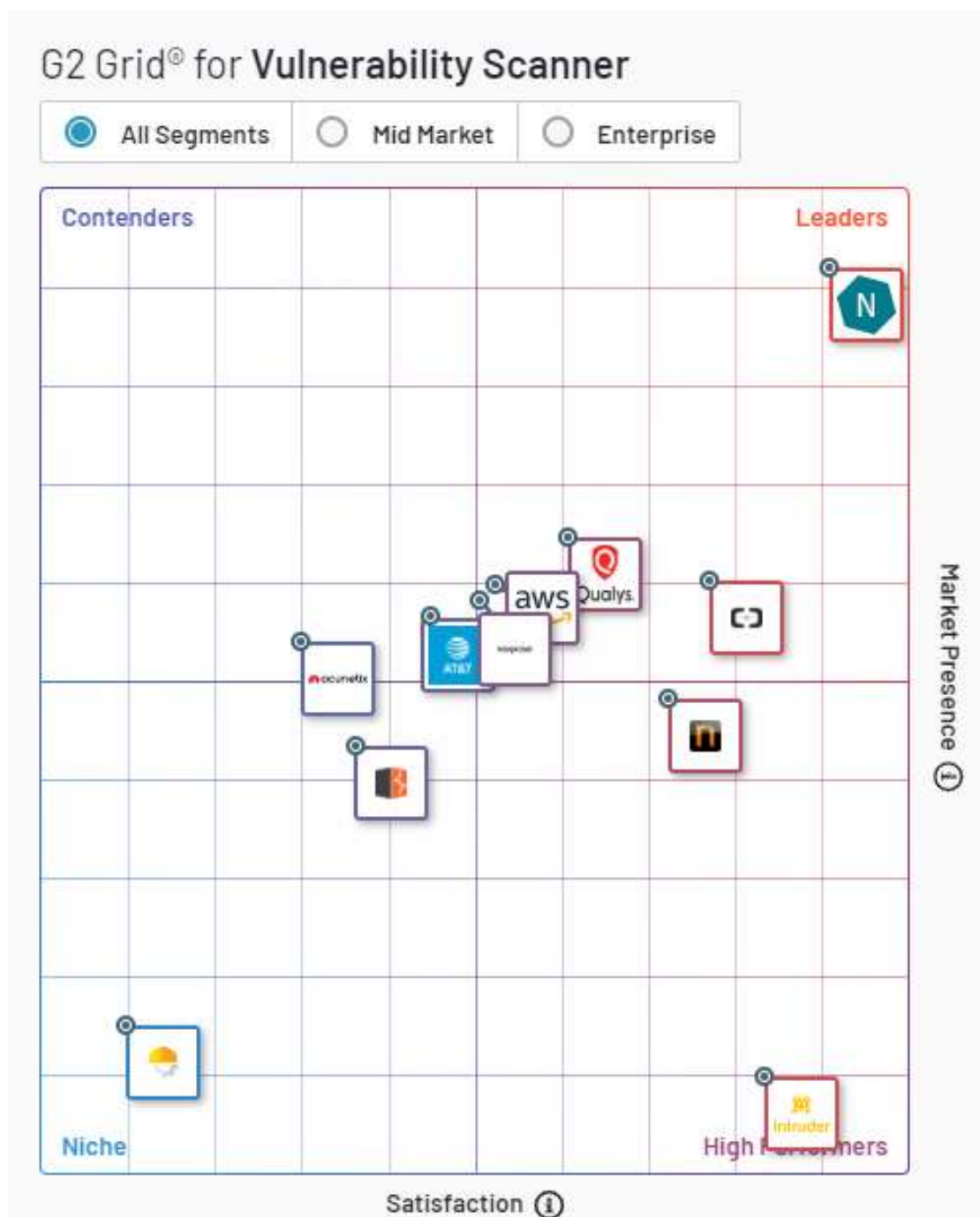


Ilustración 3 - Niveles de Satisfacción y Performance

CONCLUSIÓN

A medida que avanza el cambio de las explotaciones programadas regularmente, a la supervisión continua y las implementaciones más ágiles y descentralizadas, los métodos disponibles para detectar vulnerabilidades jugarán un papel cada vez más importante. Esto incluye la capacidad de usar un agente en activos remotos para usuarios móviles y externos, y para las arquitecturas transitorias virtualizadas y las prácticas de DevOps. Hay un movimiento constante para entregar esto desde la nube. Si bien las opciones locales aún están disponibles, el movimiento en esta dirección es innegable en términos de que los proveedores y clientes se mueven para tener más "poder de la nube" en algún lugar de su uso.

Los proveedores líderes se están moviendo para preparar sus plataformas en la nube para entregar VA. Se espera que en los próximos años, las soluciones comenzarán a ser puestas en práctica y tendrán nuevas características, aparte del soporte de contenido de seguridad de escaneo/evaluación entregado.

Las organizaciones con implementaciones en la nube, la virtualización y DevOps de gran tamaño o en crecimiento deben seleccionar una solución de VA con estos datos demográficos informáticos en mente, y deben considerar el compromiso actual y futuro de un proveedor con estas tecnologías.

En algunos casos, las brechas se cerrarán mediante la colaboración con socios tecnológicos e integraciones de terceros, en lugar del soporte nativo en las soluciones de VA. Las integraciones con los sistemas de administración de plataformas, como las suites de administración de movilidad empresarial (EMM), los hipervisores y las plataformas de seguridad en la nube, son especialmente importantes, ya que brindan mayor visibilidad y algunas capacidades de evaluación de vulnerabilidades.

Algunos proveedores del mercado también ofrecen sus soluciones VA como un componente en una cartera integrada más amplia. Dependiendo de sus requisitos, estas tecnologías combinadas pueden proporcionar una postura/solución de seguridad de mayor suma que las partes, y también ser rentables, debido a la licencia de

paquetes. Sin embargo, si no los buscan desde el principio, los potenciales beneficios implícitos no deben tentar a los posibles compradores de soluciones de VA.

Además, las siguientes capacidades son críticas, especialmente en empresas más grandes:

- Alcance, calidad y rapidez de las actualizaciones de contenido.
- Capacidad para administrar, administrar y programar escáneres y escaneos de manera centralizada
- Control de acceso basado en roles (RBAC), que admite la administración de identidades local, así como estándares como SAML que admiten soluciones de administración de acceso e identidad (IAM) locales y basadas en la nube.
- Soporte integrado para administrar y rastrear datos de vulnerabilidad, como el flujo de trabajo de administración de vulnerabilidad y la administración de tickets relacionados con la corrección de vulnerabilidad
- Soporte para nuevos tipos de servicios de nube como OT y infraestructura
- Integración con las soluciones de gestión de seguridad y flujo de trabajo empresarial, como las bases de datos de gestión de configuración (CMDB), los directorios empresariales y las soluciones de identidad e IAM.
- Opciones de arquitectura flexibles, como la implementación virtualizada y el escaneo basado en la nube
- La capacidad de automatizar el escaneo y las alertas al admitir la programación y las capacidades basadas en el flujo de trabajo.

- Gestión de excepciones para múltiples fases, escaneo, creación de tickets, informes, etc.
- Soporte para presentar API desde la herramienta VA, de modo que otras herramientas, por ejemplo, información de seguridad y gestión de eventos (SIEM); IPS; WAF; y las herramientas de seguridad, análisis y generación de informes (SOAR): pueden instrumentar y tomar información de ellos para su integración en las operaciones de seguridad.

BIBLIOGRAFÍA

- Garner. Leading research and advisory Company. Consultado 6 de junio 2019. Disponible en <https://www.gartner.com/en>
- G2. Best Vulnerability Scanner Software. Consultado 6 de Junio 2019. Disponible en <https://www.g2.com/categories/vulnerability-scanner>
- Wikipedia. La enciclopedia libre. Consultada 6 de junio 2019. Disponible en <https://es.wikipedia.org/wiki/Wikipedia:Portada>
- OBS Business School. Consultada el 6 de junio 2019. Disponible en <https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible>
- Vulnerabilidad de los sistemas informáticos. Consultada el 6 de junio 2019. Disponible en <http://vulnerabilidadtisg.blogspot.com/>
- Cero a uno. Software Corporativo. ¿Qué es un Escaneo de Vulnerabilidades?. Consultado el 6 de junio 2019. Disponible en <https://blog.cerounosoftware.com.mx/que-es-un-escaneo-de-vulnerabilidades>