Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia

Paola A. Sánchez-Sánchez^{1*}, Jose R. García- González¹, Antony Triana¹ y Leidy Perez - Coronell²

(1) Facultad de Ingenierías, Universidad Simón Bolívar, Barranquilla, Colombia.

(correo-e: psanchez9@unisimonbolivar.edu.co; jgarcia122@unisimonbolivar.edu.co; atriana@unisimon.edu.co)

(2) Facultad de Ingenierías, Corporación Universitaria Latinoamericana, Barranquilla, Colombia (correo-e: lperezc@ul.edu.co)

* Autor a quien debe ser dirigida la correspondencia.

Recibido Mar. 2, 2021; Aceptado May. 3, 2021; Versión final May. 26, 2021, Publicado Oct. 2021

Resumen

En este estudio se diseña una herramienta que permite evaluar el estado actual de vulnerabilidad informática que tiene una pequeña y mediana empresa (PYME) a partir de la medición del nivel de seguridad de su software. Se definen y describen las componentes de la herramienta que, apoyado en la base de datos de vulnerabilidades y exposiciones comunes (CVE), ofrece un mecanismo para la evaluación eficaz del riesgo cibernético y un esquema de recomendaciones. Como resultado se muestra la ejecución de cada una de las componentes de la herramienta a través del estudio de una PYME del sector de tecnología e innovación en Colombia. Se evalúa todo el software comercial en sus diferentes versiones y se sugieren líneas de acción según el nivel de riesgo calculado. Se concluye que la herramienta propuesta permite suplir las etapas iniciales de búsqueda, reporte y recomendaciones ante vulnerabilidades de riesgo cibernético, basado en un trabajo sistemático, permanente y exhaustivo, más de orden preventivo que correctivo.

Palabras clave: ciberseguridad; seguridad informática; evaluación; vulnerabilidades; exposiciones comunes

Measurement of cybersecurity risk in Colombian small and medium size enterprises (SMEs)

Abstract

The main aim of this research study is to design a tool that allows evaluating the current state of computer vulnerability in a small and medium size enterprise (SME) by measuring its software's security level. The tool's components are defined, described, and supported by the common vulnerabilities and exposures (CVE) database, which offers a solid basis for an effective cyber risk assessment and recommendation scheme. The results show the execution of each of the tool's components by assessing a Colombian information and technology SME. All commercial software is evaluated on its different versions and lines of action are suggested according to the level of calculated risk. In conclusion, the proposed tool assesses the initial stages of search, report, and recommendations for cyber risk vulnerabilities, based on a systematic, permanent, and exhaustive examination that is preventive rather than corrective.

Keywords: cybersecurity; computer security; vulnerability assessment; common exposures

INTRODUCCIÓN

Vulnerabilidad se entiende como la debilidad o exposición a ataques informáticos que pone en riesgo la seguridad de un sistema al permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la información contenida, lo que hace necesario establecer mecanismos para detectarlas y eliminarlas rápidamente (INCIBE, 2020). La exposición a vulnerabilidades informáticas es un fenómeno que ha venido presentando gran relevancia en las organizaciones debido a la creciente interconexión global. Autores como (Benz y Chatterjee, 2020; Manworren et al., 2016), afirman que todas las industrias y organizaciones, no importando el tamaño o sector son susceptibles a padecer delitos informáticos cuyos daños podrían ser del orden de U\$ 6 billones anuales para 2021. Es así como, las pequeñas y medianas empresas (pymes) son cada vez más vulnerables en términos de seguridad informática (Epps, 2017).

Las pymes se enfrentan a los mismos problemas de ciberseguridad que presentan las grandes empresas, sin embargo, la dificultad radica en que las primeras no cuentan con los recursos necesarios para abordar los riesgos de manera eficiente, y sus equipos y presupuestos de seguridad son inadecuados, por lo tanto, tienen en una desventaja significativa para lidiar con las amenazas cibernéticas (Wang et al., 2017). Las pymes suelen actuar como proveedores, contratistas y socios de organizaciones más grandes y están conectadas digitalmente. Es así como, los ciberatacantes las utilizan como puertas de enlace para vulnerar los sistemas de organizaciones más grandes. Tal como lo afirman (Shaun, 2019; Renaud, 2016), para los directivos de las pymes la ciberseguridad no es una prioridad; más aún, estos no comprenden los riesgos, y no ven a su organización como un objetivo probable, subestimando el valor de su información para la competencia, y considerando la seguridad informática un problema de las grandes empresas y no de la suya. Es así como, a menudo los directivos no justifican el gasto de recursos en ciberseguridad, lo que conduce a presupuestos insuficientes en el área (Clarke, 2015).

Los líderes de tecnología de la información y directivos de las pymes padecen de la falsa creencia que poseen una adecuada capacidad de defensa en su organización; RSM US (2018), encontró en su estudio que el 95% de las pymes encuestadas consideran que poseen mecanismos de seguridad informática superior al promedio, y su riesgo de sufrir ataques informáticos es muy bajo; sin embargo, el estado real de preparación y madurez en ciberseguridad de estas pymes puede ser bastante insatisfactorio (Tubío Figueira et al., 2020; Lloyd, 2020). Esto se evidencia en el estudio de Cyber Security Breaches Survey 2019, donde se señala que solo el 15% de las pymes poseen un proceso formal de gestión de incidentes cibernéticos, y el 50% de los líderes de TI dicen que no saben por dónde empezar para mejorar su postura de seguridad. Bajo este panorama, las organizaciones no realizan evaluaciones permanentes, sistémicas y exhaustivas del riesgo cibernético (Schuh et al., 2020; Nenekazi y Zubeida, 2020).

Para el caso de Colombia, (Martínez Cortes, 2015) destaca el riesgo de seguridad informática de las pymes en Colombia y afirma que los errores comunes que se comenten al interior de las instituciones en materia de seguridad informática son, entre otros: no valorar la información, considerar que la seguridad equivale a un antivirus, y confiar en tecnología no adecuada. Así mismo, (Mardini y Egea, 2017; Monsalve-Pulido, 2014; Ospina y Sanabria, 2020) ratifican la importancia de los mecanismos de ciberseguridad para todas las organizaciones e instituciones que hoy en día ejecutan sus funciones mediante el tratamiento de datos. Por lo tanto, todos concuerdan en que las pymes en Colombia son altamente vulnerables a riesgos en seguridad informática y es necesaria una adecuada gestión de estos (Franco, 2013). Ahora bien, cada día surgen nuevas vulnerabilidades que afectan todo tipo de programas, servicios y sistemas operativos, las cuales son agregadas a las bases de datos específicas. "The MITRE Corporation", cuenta con una base de datos de vulnerabilidades denominada CVE (Common Vulnerabilities and Exposures), que permite identificar debilidades en un producto, al proporcionar identificadores estandarizados para cada vulnerabilidad o exposición. Sin embargo, aunque existen este tipo de bases de datos, a menudo las organizaciones de pequeño y mediano tamaño no están permanentemente al margen de ellas, teniendo brechas de seguridad.

El objetivo de este artículo es el diseño de una herramienta de software que i) realiza una búsqueda automática exhaustiva de vulnerabilidades y exposiciones riesgosas, a través de un proceso riguroso de identificación de todos los paquetes de software instalados en sistemas, servidores, computadores portátiles, máquinas virtuales, dispositivos móviles y computadores de escritorio, ii) contrasta las vulnerabilidades en diferentes bases de datos compatibles con CVE, iii) notifica el tipo de vulnerabilidad y el nivel de riesgo de la organización, y iv) sugiere algunas acciones a ejecutar para mitigarlo o eliminarlo. La herramienta propuesta permite a una pequeña o mediana organización dar respuesta a los siguientes interrogantes (Kaila y Nyman, 2018): ¿A cuáles vulnerabilidades cibernéticas está expuesta mi organización?, ¿Cuál es el nivel de riesgo de cada vulnerabilidad en mi organización?, ¿Cuál es el nivel de riesgo aceptable de cada vulnerabilidad?, ¿Qué acciones podemos ejecutar para mitigar o eliminar los riesgos cibernéticos?

La ineficaz gestión de riesgos cibernéticos de las organizaciones conduce frecuentemente a impactos económicos representativos, por lo tanto, se requiere un trabajo sistemático, permanente y exhaustivo

más de orden preventivo que correctivo, que permita evaluar la vulnerabilidad a riesgos cibernéticos y entablar acciones para controlarlos (Zuñá, 2019; Martins y Oliveira, 2019). La evaluación de vulnerabilidades es el proceso de identificar, cuantificar y priorizar (o clasificar) las debilidades de seguridad en un sistema informático (Sabillón y Cano, 2019; González y Montesino, 2018).

En esta investigación se propone una herramienta para la medición de vulnerabilidades de riesgo cibernético en pymes apoyado en la base de datos CVE, la cual ofrece una base sólida para hacer una evaluación eficaz y ofrecer un esquema de recomendaciones. CVE proporciona información sobre vulnerabilidades y amenazas públicas reconocidas, las cuales se resumen en una puntuación numérica conocida como Common Vulnerability Score System (CVSS) (CVSS, 2019), que refleja sus principales características y su gravedad. Esta puntuación numérica se puede traducir en una representación cualitativa (como baja, media, alta o crítica) para ayudar a evaluar y priorizar las vulnerabilidades en los procesos de gestión de vulnerabilidades derivados del análisis de riesgos.

METODOLOGÍA

Teniendo en cuenta que la lista de vulnerabilidades está relacionada con el software que posee la organización y su versión, en esta investigación se seleccionaron los paquetes de software comerciales comúnmente usados en las pymes en Colombia. La estrategia propuesta para la especificación y construcción de una herramienta para la búsqueda de vulnerabilidades cibernéticas en pymes considera un proceso sistémico y sistemático cuya definición y declaración inicial corresponde con el planteamiento de un proyecto de investigación (García-González y Sánchez-Sánchez, 2020). El modelo sistémico de la herramienta se esquematiza en la Figura 1, el código fuente de la herramienta puede consultarse en el repositorio (Sánchez-Sánchez, 2020).

Fig. 1: Esquema de herramienta para búsqueda de vulnerabilidades cibernéticas en pymes.

Selección de equipos: este proceso hace referencia a la etapa inicial de selección de equipos y dispositivos dentro de la pyme que serán susceptibles para el análisis. Se recomienda que la evaluación se realice en la totalidad de los equipos, especialmente si estos se encuentran enlazados a través de una red, esto incluye: sistemas, servidores, computadores portátiles, máquinas virtuales, dispositivos móviles y computadores de escritorio.

Búsqueda de vulnerabilidades: este proceso es el corazón de la herramienta desarrollada, y se basa en el uso de agentes de búsqueda inteligente que identifican en cada uno de los equipos y dispositivos seleccionados el software instalado, sus versiones y a partir de esto realiza una búsqueda de vulnerabilidades en CVE para cada uno de ellos. El objetivo de este proceso es elaborar una lista completa de las vulnerabilidades de las diferentes aplicaciones instaladas en cada equipo. CVE Details (CVSS, 2019) reúne las mayores vulnerabilidades que encuentran los proveedores de softwares, hardware e investigadores, registrándolas bajo un estándar en la que cada referencia tiene un número de identificación CVE-ID, una descripción de la vulnerabilidad, las versiones del software afectadas, y una posible solución. No obstante, CVE Details no posee API de consulta automática, por lo que la consulta se hace uno a uno, por lo tanto, se requiere un proceso automático que realice la evaluación de la totalidad de programas instalados en cada equipo seleccionado. Para la automatización del proceso de búsqueda se requirió el uso de un agente inteligente con tres componentes: captura de lista de programas de software, consulta en

diccionario unificado de nombres y Web Scraping, el cual se esquematiza en la Figura 2. El agente inteligente realiza en primer lugar la consulta de los programas instalados en los equipos seleccionados. El insumo de consulta inicial entrega un listado con el nombre de los programas instalados, versión y proveedor.

Fig. 2: Agente inteligente para búsqueda de vulnerabilidades.

La consulta de los programas instalados se basa en el idioma y arquitectura del sistema operativo, por lo tanto, a menudo el nombre del programa no coincide con el registro en CVEDetails.com. Por lo tanto, se hace necesario un estándar que permita hacer una referencia única al nombre de cada software en las diversas plataformas y de un mecanismo orientado a la comparación de los nombres de los softwares. Con los objetivos enunciados se creó un diccionario de nombres unificados basado en el diccionario oficial de Enumeración de Plataforma Común, CPE (Common Platform Enumeration). Ver ejemplo en Tabla 1. La construcción del diccionario se basó en el top de los 100 programas de software comercial más utilizados por las pymes en Colombia. En este proceso el resultado de la consulta inicial es comparado con el diccionario unificado el cual ofrece como salida el nombre CPE del software. Finalmente, se realiza un proceso de Web scraping donde se hace la consulta y extracción de información del sitio web de CVE Details.

Tabla 1: Ejemplo de campos en diccionario de nombres

Nombre generado en búsqueda	Microsoft Word MUI (Español) 32 Bits 2020
Nombre en CPE	Word

Identificación de riesgos: este proceso consiste en la extracción de información de riesgos asociados a cada uno de los programas y versiones consultados en el proceso de búsqueda de vulnerabilidades. El objetivo de este proceso es la priorización de vulnerabilidades, la cual implica la asignación de un rango o puntuación de gravedad a cada vulnerabilidad, en función de factores como: sistemas que se ven afectados, datos en riesgo, funciones comerciales en riesgo, facilidad de ataque o compromiso, severidad de un ataque, daños potenciales como resultado de la vulnerabilidad, etc. El rango de medición de riesgo de vulnerabilidades usado está en una escala de 0 a 10, ver Figura 3, y se basa en el estándar CVSS que presenta una puntuación y una escala cualitativa del impacto y severidad de las vulnerabilidades.

CVSS Sscore	Severidad
0-1	Nula
1-2	
2-3	
3-4	Baja
4-5	
5-6	Media
6-7	
7-8	Alta
8-9	
9-10	Crítica

Fig. 3: Escala de nivel de seguridad de un producto. Fuente: (CVSS, 2019)

Reporte de vulnerabilidades: el objetivo de este proceso es hacer un reporte resumido del riesgo de cada programa. En caso de que no se encuentren vulnerabilidades en la versión del programa, se hace una búsqueda en versiones más recientes (si las hay), bajo la premisa que vulnerabilidades en versiones

recientes afectan en igual o mayor grado los programas, por lo tanto, tiene un nivel de riesgo igual a su versión reciente. Una vez analizada la versión del programa, la herramienta muestra el número total de vulnerabilidades encontradas, el valor promedio de vulnerabilidad o del nivel de seguridad del producto y la severidad asociada al promedio medido en la escala de la Figura 3. En caso de no encontrar vulnerabilidades asociadas al programa, ni versiones más recientes, la herramienta exhibe la leyenda “No existen vulnerabilidades para este producto”.

Informe detallado y recomendaciones: en el reporte de vulnerabilidades se hace un resumen general de cada programa evaluado en los equipos, sin embargo, con el fin de aplicar medidas correctivas y preventivas, es necesario un proceso detallado de cada vulnerabilidad, donde se describa el impacto de cada amenaza, se priorice las vulnerabilidades en función de la gravedad, la antigüedad, el código de explotación, la divulgación y la disponibilidad de parches, y se establezcan recomendaciones para mitigar o prevenir. El informe detallado se presenta en un archivo en formato .csv y está organizado por fecha de publicación de la vulnerabilidad de forma descendente, es decir de la más reciente a la más antigua.

RESULTADOS Y DISCUSIÓN

Con el fin de mostrar el funcionamiento de cada proceso de la herramienta propuesta se hizo la prueba en un equipo perteneciente a una pyme del sector TI. En este apartado se presenta un análisis y discusión de las etapas declaradas en la Figura 1 para el caso de aplicación. En las etapas iniciales se hace la selección del equipo y el análisis de vulnerabilidades. A continuación, se enuncia la sucesión detallada de procesos de ambas etapas: 1) Se elige un equipo para la ejecución de la herramienta; 2) Se realiza un escaneo de los programas instalados en el equipo; 3) Se produce un listado de programas instalados; 4) Se verifica el nombre del programa en el diccionario de nombres; 5) Se consulta y extrae información del sitio CVE Details y 6) Se despliega en pantalla la respuesta a cada proceso enunciado. En la Figura 4 se presenta una porción de la captura de pantalla que da cuenta de las salidas en las primeras etapas de ejecución de la herramienta.

```
[*] Iniciando escaneo...

[*] Programa --> .net Framework
[*] Versión --> 4.5.50932
[*] Buscando para ".net Framework 4.5.50932" en cvedetails.com
[!] No hay una coincidencia exacta para este producto/versión. Comprobando si hay
    CVE en las nuevas versiones...
[+] La versión superior más cercana que se encuentra en la base de datos es: 4.6
[*] Resumen de IDs: Vendor=Microsoft [26] | Product=.net Framework [2002] |
    Version=4.6 [185326]
[*] Obtener los resultados de la versión --> ID: 185326 ...
[+] Número total de CVEs que se han obtenido: 30
[+] Promedio de vulnerabilidades: 5.739999999999999
[+] Severidad de vulnerabilidades: Media
[*] Para más detalle consulte el archivo '.net Framework.csv' en la carpeta
    reportes

[*] Programa --> Mysql Workbench
[*] Versión --> 8.0.20
[*] Buscando para "Mysql Workbench 8.0.20" en cvedetails.com
[!] No hay una coincidencia exacta para este producto/versión. Comprobando si hay
    CVE en las nuevas versiones...
[!] No se ha encontrado una versión superior en la base de datos de
    cvedetails.com
[*] No existen vulnerabilidades para este producto

[*] Programa --> Office
[*] Versión --> 16.0.12730.20250
[*] Buscando para "Office 16.0.12730.20250" en cvedetails.com
[!] No hay una coincidencia exacta para este producto/versión. Comprobando si hay
    CVE en las nuevas versiones...
[!] No se ha encontrado una versión superior en la base de datos de
    cvedetails.com
[*] No existen vulnerabilidades para este producto
```

Fig. 4: Captura de pantalla de ejecución de la herramienta.

Tal como se muestra en la figura 4, en el proceso de búsqueda de vulnerabilidades, el primer programa que encuentra y escanea es .net Framework bajo la versión 4.5.50932. Específicamente para esta versión no se registran vulnerabilidades en CVE Details.com, por lo cual la herramienta inicia una búsqueda en

versiones superiores a esta. En este caso encuentra vulnerabilidades registradas bajo la versión 4.6. Para la versión superior encontrada se hace un reporte resumido de las vulnerabilidades, donde se indica número total, valor promedio de riesgo de vulnerabilidades y la severidad asociada. El número de vulnerabilidades encontradas para el programa .net Framework es de 30, con un promedio de riesgo de 5.74 lo cual equivale a una severidad Media.

La herramienta genera en la carpeta reporte un archivo .csv de informe detallado y recomendaciones, donde cada una de las 30 vulnerabilidades son descritas, se valora su impacto y se ofrece una recomendación. La Figura 5 muestra una porción de la captura de pantalla del informe detallado de vulnerabilidades para el programa .net Framework. Los campos incluidos en el reporte son: ID - identificación de la vulnerabilidad según estándar de vulnerabilidades CVE; CVSS - escala de riesgo CVSS en valor numérico y color; Date - fecha de última actualización de la vulnerabilidad; Description - descripción de la vulnerabilidad; URL - enlace a sitio web de consulta ampliada de la vulnerabilidad.

ID	CVSS	Date	Description	URL
CVE-2019-1142	2,10	11/09/2019	An elevation of privilege vulnerability exists when the .NET Framework common language runtime (CLR) allows file creation in arbitrary locations, aka ".NET Framework Elevation of Privilege Vulnerability".	http://www.cvedetails.com/cve/CVE-2019-1142/
CVE-2019-1113	6,80	15/07/2019	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka ".NET Framework Remote Code Execution Vulnerability".	http://www.cvedetails.com/cve/CVE-2019-1113/
CVE-2019-1083	5,00	15/07/2019	A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests, aka ".NET Denial of Service Vulnerability".	http://www.cvedetails.com/cve/CVE-2019-1083/
CVE-2019-1006	5,00	15/07/2019	An authentication bypass vulnerability exists in Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allowing signing of SAML tokens with arbitrary symmetric keys, aka "WCF/WIF SAML Token Authentication Bypass Vulnerability".	http://www.cvedetails.com/cve/CVE-2019-1006/
CVE-2019-0981	5,00	16/05/2019	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka ".NET Framework and .NET Core Denial of Service Vulnerability". This CVE ID is unique from CVE-2019-0820, CVE-2019-0980.	http://www.cvedetails.com/cve/CVE-2019-0981/
CVE-2019-0980	5,00	16/05/2019	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka ".NET Framework and .NET Core Denial of Service Vulnerability". This CVE ID is unique from CVE-2019-0820, CVE-2019-0981.	http://www.cvedetails.com/cve/CVE-2019-0980/
CVE-2019-0864	2,10	16/05/2019	A denial of service vulnerability exists when .NET Framework improperly handles objects in heap memory, aka ".NET Framework Denial of Service Vulnerability".	http://www.cvedetails.com/cve/CVE-2019-0864/
CVE-2019-0820	5,00	16/05/2019	A denial of service vulnerability exists when .NET Framework and .NET Core improperly process RegEx strings, aka ".NET Framework and .NET Core Denial of Service Vulnerability". This CVE ID is unique from CVE-2019-0980, CVE-2019-0981.	
			An information disclosure vulnerability exists in .NET Framework which allows bypassing Cross-origin Resource Sharing (CORS) headers.	

Fig. 5. Captura de pantalla de informe detallado de ejecución de la herramienta en programa .net Framework.

El reporte detallado del programa .NET Framework permite identificar una vulnerabilidad con severidad media registrada bajo CVE-2019-1113, de la cual se ofrece una descripción en el archivo; así mismo, al ahondar en el detalle, mostrado en la Figura 6, se observa que existe una vulnerabilidad de ejecución remota de código en el software .NET cuando el software no puede verificar el código fuente de un archivo. Un atacante que explote con éxito la vulnerabilidad podría ejecutar un código arbitrario en el contexto del usuario actual. Lo anterior implica que, si el usuario actual inicia sesión con derechos de administrador, se expone a que un atacante tome el control del sistema, y de esta forma, podría ver, cambiar o eliminar datos; instalar programas; o crear cuentas con todos los derechos del usuario actual. Los usuarios con derechos limitados tienen menos afectación. Esta vulnerabilidad también se conoce como ".NET Framework Remote Code Execution Vulnerability" (CVE Details 2019-1113).

Este ataque a la seguridad del sistema ocurre cuando el usuario abre un archivo corrupto (archivo especialmente diseñado con una versión afectada de .NET Framework) que puede ser recibido vía correo electrónico. La exposición a la vulnerabilidad afecta parcialmente la integridad del sistema, la confidencialidad y la disponibilidad. La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que .NET Framework verifica el marcado de origen de los archivos. La totalidad de las vulnerabilidades, no importando su nivel de criticidad, pueden ser consultadas a través del enlace URL que se genera para cada una, el cual, como en el caso expuesto en la Figura 6, ofrece la descripción de la vulnerabilidad y recomendaciones orientadas a resolverla o mitigarla. Los enlaces URL son generados automáticamente con el reporte detallado y se dirigen al sitio web de CVE Details que corresponde con cada vulnerabilidad identificada.

Vulnerability Details : [CVE-2019-1113](#)

A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka '.NET Framework Remote Code Execution Vulnerability'.

Publish Date : 2019-07-15 Last Update Date : 2019-07-19

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	6.8
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

Fig. 6: Informe detallado de descripción de vulnerabilidad CVE-2019-1113 en ejecución de la herramienta para el programa .net Framework.

CONCLUSIONES

La evaluación de vulnerabilidades informáticas es un proceso que ha venido demandando gran atención en las organizaciones debido a la exposición permanente a delitos cibernéticos. En este trabajo se presenta el diseño de una herramienta que permite suplir las etapas iniciales de búsqueda, reporte y recomendaciones de vulnerabilidades y exposiciones, cuyo potencial solo ha sido desarrollado de manera incipiente. La herramienta y procesos descritos en este documento pueden constituir un entorno de experimentación valioso para las pymes en términos de agilidad, eficacia y eficiencia, donde se resaltan las siguientes ventajas: La herramienta genera una base de datos de vulnerabilidades y la aplicación de técnicas de auditoría, que permite a las pymes anticiparse ante ataques informáticos. La herramienta no limita el número de consultas semanales o mensuales, dando libertad al encargado de TI de realizar evaluaciones cuando lo considere necesario y en un número ilimitado de equipos. La mayoría de las herramientas comerciales de evaluación de vulnerabilidades establecen un máximo de consultas. La herramienta puede permitir reducir eficazmente los fallos de seguridad más comunes de un sistema. Se convierte en una alarma a los problemas de seguridad y/o configuración que pueden no ser tenidos en cuenta por un administrador de sistemas o a un gestor de seguridad informática. La herramienta ayuda a las pymes a atender el riesgo en el que están expuesto y facilita la disminución de las vulnerabilidades. La comprensión de las vulnerabilidades potenciales por medio de la herramienta fortalece la estrategia de seguridad de la organización.

REFERENCIAS

- Benz, M., y Chatterjee, D., Calculated risk? A cybersecurity evaluation tool for SMEs, <https://doi.org/10.1016/j.bushor.2020.03.010>, Business Horizons, 63(4), 531–540 (2020)
- Clarke, R., The prospects of easier security for small organizations and consumers, <https://doi.org/10.1016/j.clsr.2015.05.004>, Computer Law & Security Review, 31(4), 538–552 (2015)
- CVSS., Common Vulnerability Scoring System, V4.0 Development Update, First.org, Inc., 2019. <https://www.first.org/cvss/> (2019)
- Epps, C., Best practices to deal with top cybercrime activities, [https://doi.org/10.1016/S1361-3723\(17\)30032-5](https://doi.org/10.1016/S1361-3723(17)30032-5), Computer Fraud & Security, 2017(4), 13–15 (2017)
- Franco, D.A., Perea, J.L., y Tovar, L.C., Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios, <https://doi.org/10.4067/S0718-07642013000500003>, Información Tecnológica, 24(5), 13–22 (2013)

- García-González, J.R., y Sánchez-Sánchez, P.A., Diseño teórico de la investigación: instrucciones metodológicas para el desarrollo de propuestas y proyectos de investigación científica, <https://dx.doi.org/10.4067/S0718-07642020000600159>, Información Tecnológica, 31(6), 159-170 (2020)
- González, H., y Montesino, R., Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web, Revista Cubana de Ciencias Informáticas, 12(4), 52-65. (2018)
- INCIBE, Amenaza vs vulnerabilidad: cómo diferenciarlos, Instituto nacional de ciberseguridad-INCIBE, España, 22 Dic 2020, <https://www.incibe.es/> (2020).
- Lloyd, G., The business benefits of cyber security for SMEs, [https://doi.org/10.1016/S1361-3723\(20\)30019-1](https://doi.org/10.1016/S1361-3723(20)30019-1), Computer Fraud & Security, 2020 (2), 14–17 (2020)
- Kaila, U., y Nyman, L., Information Security Best Practices: First Steps for Startups and SMEs, <https://doi.org/10.22215/timreview/1198>, Technology innovation management review, 8(11), 32–42 (2018)
- Manworren, N., Letwat, J., y Daily, O., Why you should care about the Target data breach, <https://doi.org/10.1016/j.bushor.2016.01.002>, Business Horizons, 59(3), 257–266 (2016)
- Mardini, J., y Egea, A., Modelo de detección de intrusiones en sistemas computacionales, realizando selección de características con chi square, entrenamiento y clasificación con ghsom, <https://doi.org/10.17081/invinno.5.1.2614>, Investigación e Innovación en Ingenierías, 5 (1), 24–35 (2017)
- Martínez-Cortés J.F., Seguridad de la Información en pequeñas y medianas empresas (pymes), Universidad Piloto de Colombia., 8 (2015)
- Martins, T., y Oliveira, S.V.G., Cybersecurity in the Power Electronics, <https://doi.org/10.1109/TLA.2019.8932339>, IEEE Latin America Transactions, 17(8), 1300–1308 (2019)
- Monsalve-Pulido, J.A., Aponte-Novoa, F.A., y Chaves-Tamayo, D.F., Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia), <https://doi.org/10.19053/01211129.2791>, Revista Facultad de Ingeniería, 23(37), 65-66 (2014)
- Nenekazi, M., y Zubeida, K., Cyber-Threat Information-Sharing Standards: A Review of Evaluation Literature, <https://dx.doi.org/10.23962/10539/29191>, The African Journal of Information and Communication, 25, 1-12. (2020)
- Ospina, M., y Sanabria, P., Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia, Revista Criminalidad, 62(2), 199-217 (2020)
- Renaud, K., How smaller businesses struggle with security advice, [https://doi.org/10.1016/S1361-3723\(16\)30062-8](https://doi.org/10.1016/S1361-3723(16)30062-8), Computer Fraud & Security, 8, 10–18 (2016)
- RSM US LLP., Middle market businesses advance cybersecurity protections but might underestimate risk, RSM survey finds, PR Newswire, 15 May 2018, <https://www.prnewswire.com/> (2018).
- Sabillón, R., y Cano, J., Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones, <https://dx.doi.org/10.17013/risti.32.33-48>, RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (32), 33-48 (2019)
- Sánchez-Sánchez P.A., GitHub: Measurement of the level of IT security in SMEs. 2020. <https://github.com/> (2020).
- Schuh, G., Hicking, J., y otros tres autores, Helping companies to evaluate their status quo in information security with a serious gaming-based economical quantification approach, <https://doi.org/10.1016/j.procir.2020.05.196>, Procedia CIRP, 93, 587–592 (2020)
- Shaun, W., Integrated framework for information security investment and cyber insurance, <https://doi.org/10.1016/j.pacfin.2019.101173>, Pacific-Basin Finance Journal, 57, 1-12 (2019)
- Tubío Figueira, P., López Bravo, C., y Rivas López, J.L., Improving information security risk analysis by including threat-occurrence predictive models, <https://doi.org/10.1016/j.cose.2019.101609>, Computers & Security, 88 (2020)
- Wang, Y., Anokhin, O., y Anderl, R., Concept and use Case Driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0, <https://doi.org/10.1016/j.procir.2017.03.142>, Procedia CIRP, 63, 207–212 (2017)
- Zuñiga Macancela, C.J., Arce Ramírez, E.R., Romero Berrones, Á., y Soledispa Baque, W.J., Análisis de la seguridad de la información en las pymes de la ciudad de Milagro, Revista Universidad y Sociedad, 9(2), 313–318 (2019)