Ciencia e Ingeniería Neogranadina 2024 Vol. 34(1) enero-junio ■ ISSN: 0124-8170 · e-ISSN: 1909-7735 ■ pp. 11-22

Editorial Neogranadina

DOI : https://doi.org/10.18359/rcin.7059

Bug-Bounty, ¿el futuro del *pentesting*?*

Jaime Andrés Restrepo-Gómez[a] ■ Luis Carlos Correa-Ortiz[b]

Resumen: Al comienzo del artículo se ofrece un resumen de los desafíos contemporáneos que enfrentan las corporaciones con respecto a la protección de datos. Luego se expone una táctica efectiva para las entidades: la implementación de auditorías de seguridad y ejercicios de intrusión controlada, enfocándose en el análisis a profundidad de dos de estas: los cuestionarios de penetración (*pentesting*) y el *Bug-Bounty*, con sus definiciones y sus evoluciones, como sus ventajas y desventajas. Finalmente, se argumenta que el *Bug-Bounty* no puede reemplazar completamente al *pentesting* realizado por expertos, y pueden verse como dos enfoques complementarios que podrían ayudar a mejorar la seguridad de una organización.

Palabras clave: *Bug-Bounty*; pruebas de penetración (*pentesting*); seguridad de la información; investigadores en seguridad.

Recibido: 14/11/2023.

Aceptado: 28/02/2024.

Disponible en línea: 30/06/2024.

Cómo citar: J. A. Restrepo-Gómez y L. C. Correa-Ortiz «Bug-Bounty, ¿el futuro del Pentesting?», Cien. Ing.Neogranadina, vol. 34, n.º 1, pp. 11–22.

* Artículo de reflexión proveniente del proyecto *Análisis de Bug-Bounty más allá del Pentesting*, ejecutado en el periodo enero 2021-diciembre 2022, como opción de grado para optar el título de magíster en seguridad de la información.

a Ingeniero de sistemas y telecomunicaciones. CEO DragonJAR. Magíster en seguridad de la información, Universidad de Manizales (Manizales, Caldas Colombia).
Correo electrónico: jarestrepo25397@umanizales.edu.co
ORCID: https://orcid.org/0009-0000-2256-8201

b Magíster en ingeniería. Magíster en educación y desarrollo humano. Ingeniero electrónico. Profesor asociado de la Facultad de Ciencias e Ingeniería de la Universidad de Manizales (Manizales, Caldas, Colombia).
Correo electrónico: lcco@umanizales.edu.co
ORCID: https://orcid.org/0000-0001-9488-5249

Bug-Bounty, the Future of Pentesting?

Abstract: At the beginning of the article, a summary of the contemporary challenges facing corporations regarding data protection is provided. Then an effective tactic for entities is exposed: the implementation of security audits and controlled intrusion exercises, focusing on the in-depth analysis of two of these: penetration testing (*pentesting*) and *Bug-Bounty*, with their definitions and their evolutions, such as their advantages and disadvantages. Finally, it is argued that *Bug-Bounty* cannot completely replace expert-led *pentesting*, and they can be seen as two complementary approaches that can help improve an organization's security.

Keywords: *Bug-Bounty*; Penetration Testing (*Pentesting*); Information Security; Security Researchers

Bug-Bounty, o futuro do pentesting?

Resumo: No início do artigo, é oferecido um resumo dos desafios contemporâneos que as corporações enfrentam em relação à proteção de dados. Em seguida, expõe-se uma tática eficaz para as entidades: a implementação de auditorias de segurança e exercícios de intrusão controlada, focando-se na análise aprofundada de dois destes: os questionários de penetração (*pentesting*) e o *Bug-Bounty*, com suas definições e evoluções, bem como suas vantagens e desvantagens. Finalmente, argumenta-se que o *Bug-Bounty* não pode substituir completamente o *pentesting* realizado por especialistas, e é possível observá-los como dois enfoques complementares que podem ajudar a melhorar a segurança de uma organização.

Palavras-chave: *Bug-Bounty*; testes de penetração (*pentesting*); segurança da informação; pesquisadores de segurança

Introducción

Entre los obstáculos significativos que las entidades corporativas deben manejar hoy día se encuentra la salvaguarda integral de su información. La pérdida o secuestro de datos puede afectar a cualquier organización o individuo en términos de su reputación, sus finanzas y la posibilidad de perder recursos. *IT Governance* ha identificado cinco principales riesgos para las organizaciones en el Reino Unido, que van desde la falta de instalación oportuna de actualizaciones de *software* (parches) hasta la suplantación de identidad (*phishing*), contraseñas débiles, secuestro de datos (*ransomware*) y otras formas de *malware*. En Colombia, también se han reconocido dichos peligros, considerando, por ejemplo, las consecuencias del *software* de secuestro (*ransomware*), vulneración mediante códigos QR, uso de tecnología *deepfake* para clonar, de troyanos para la recopilación de información y ataques de *business email compromise*. Resulta crucial que las entidades adopten acciones preventivas frente a estas amenazas, para asegurar su resiliencia y mantener la seguridad de sus datos e información. Esto puede comprender la adopción de salvaguardas apropiadas, tales como contraseñas seguras y sistemas de autenticación multifactor, y la ejecución periódica de pruebas de intrusión para detectar y mitigar fallos en sus infraestructuras digitales. También es importante educar a los empleados sobre cómo identificar y prevenir potenciales amenazas, tales como los engaños de suplantación de identidad en línea (*phishing*) o el *malware*. De esta manera, las organizaciones pueden protegerse contra posibles ataques y garantizar la seguridad de sus datos e información [1], [2], [3], [4].

Estas organizaciones pueden adoptar una postura ofensiva frente a estos riesgos mediante la realización de evaluaciones de vulnerabilidades y pruebas de intrusión, conocidas como Evaluación de vulnerabilidades y pruebas de penetración (VAPT por sus siglas en inglés), con profesionales y empresas dedicadas a la seguridad de la información [1]. La evaluación de vulnerabilidades (VA, por sus siglas en inglés) es un proceso para detectar, clasificar y evaluar las debilidades de seguridad en el sistema objetivo (por ejemplo, una página web) mediante inspecciones automatizadas. Las pruebas de penetración (PT por sus siglas en inglés) implican la explotación activa de dichas vulnerabilidades, para determinar su gravedad y el potencial de daño que pueden causar [5], [6].

Muchas veces, asumir posturas ofensivas con iniciativas internas y con aliados externos, como terceros que realicen pruebas de penetración, no es suficiente, ya que suelen estar limitados por el tiempo y por las habilidades técnicas de un grupo pequeño de personas asignadas a esta tarea. Es por eso que cada vez más organizaciones catalogadas como maduras en procesos de seguridad informática han eliminado la mayoría de problemas de seguridad por medio de dichos procesos y han recogido las famosas frutas bajas (*low hanging fruits*), crean programas, ya sean de forma particular o a través de una plataforma especializada, para encontrar todos esos problemas de seguridad que sus ejercicios de VAPT no han detectado por su complejidad y dificultad de ejecución [7].

El presente artículo busca exponer los fundamentos tanto del *Bug-Bounty* como del *pentesting* y reflexionar sobre estas dos alternativas, como elemento de discusión en la toma de decisiones por parte de las organizaciones al momento de implementar cualquiera de estas iniciativas, y como una contribución al área de la seguridad de la información, en la que los beneficios y las problemáticas de ambas iniciativas se han analizado de forma independiente, más no conjunta.

¿Qué es *pentesting*?

El examen de intrusión o también llamado Prueba de *pentesting* se refiere al proceso de evaluación de la seguridad y a la detección de puntos débiles en un sistema informático. Es utilizado por las organizaciones para poner a prueba los controles de seguridad implementados y validar los posibles problemas de seguridad que puedan tener sus activos digitales [8]. Las pruebas de penetración a menudo las realiza un profesional de seguridad capacitado que intentará obtener acceso a la red de un sistema e identificar los puntos débiles [9].

El proceso de *pentesting* simula un ataque real y consiste en que una persona o grupo de expertos en seguridad informática se ponen en el papel de un delincuente informático y examinan los activos informáticos de una organización. Esto se hace para identificar y corregir problemas de seguridad de forma proactiva y evitar que personas malintencionadas puedan aprovecharse de ellos [10]. Así las entidades pueden reforzar la seguridad de sus sistemas informáticos y resguardarse ante posibles incursiones maliciosas.

El *pentesting* puede ser realizado con distintos tipos de alcances, conocidos como cajas, y con distintos colores (blanco, gris y negro); estos colores vienen del ambiente *hacker*, que a su vez los toma del mundo de las películas a blanco y negro, en las que por las limitantes de su tecnología y para facilitar el entendimiento de los espectadores, les asignaban un sombrero blanco al "bueno" de la película, un sombrero negro al "malo" y un sombrero gris a quien durante la trama iniciaba como un personaje "bueno" que cambiaba de parecer a un personaje "malo" o viceversa [11]. Trasladado al entorno del *pentesting*, la caja blanca se usa cuando el equipo auditor tiene pleno conocimiento de los activos a auditar, cuenta con usuarios y acceso completo a dichos activos; la caja gris, cuando se cuenta con alguna información del entorno, por ejemplo, sin usuarios o con usuarios de bajos privilegios, y la caja negra, cuando el equipo auditor no tiene mayor conocimiento sobre el entorno a auditar y debe recabar esta información por su cuenta [11].

El proceso de *pentesting* tiene como resultado final una serie de informes. El principal es el informe técnico, que debe incluir detalles sobre cada uno de los problemas de seguridad identificados, así como los próximos pasos necesarios para validar y reparar las vulnerabilidades encontradas. Además, se debe entregar un informe ejecutivo que resuma de manera clara y concisa el impacto que cada problema identificado podría tener en la organización. Esto es importante para que los directivos puedan tomar decisiones basados en esta información [9].

El *pentesting* es importante para las organizaciones empresariales, porque les permite determinar la efectividad de sus medidas de seguridad e identificar sus debilidades. El nivel de madurez en seguridad informática de una organización puede variar, dependiendo del tamaño, tipo y complejidad de su infraestructura de tecnología y datos. Sin embargo, realizar pruebas de penetración de forma regular y validarlas con terceros experimentados es fundamental para mejorar el nivel de madurez en seguridad de una empresa [12].

Bug-Bounty: definición

El concepto de recompensas por errores (*Bug-Bounty*) surge de su propio nombre. *Bug* se refiere a un fallo o problema en un *software* o *hardware*, mientras que *Bounty* alude a una recompensa otorgada a quien identifica el fallo. Un programa de recompensas por errores es un acuerdo entre una organización y auditores de seguridad de todo el mundo, en el cual la organización ofrece su infraestructura tecnológica y activos digitales para que los auditores busquen fallas a cambio de una remuneración económica o de otro tipo [13]. De esta manera, las organizaciones pueden mejorar la seguridad de sus sistemas y protegerse contra posibles ataques.

Los inicios del *Bug-Bounty*

La práctica del *Bug-Bounty* no es una novedad. Uno de los prototipos más representativos es el del matemático y científico de la computación Donald Knuth, autor de *The Art of Computer Programming,* un texto fundamental en la ingeniería de *software*. En 1964, Knuth asumió que su libro no estaría exento de fallos, por lo que invitó a los lectores a señalar cualquier error, ofreciendo una recompensa de 256 centavos de dólar por cada error encontrado [14]. Con el tiempo, el cheque ofrecido se ha convertido en un objeto de colección más que en un incentivo monetario, destacando a Knuth como uno de los pioneros en la instauración de un programa de recompensas por errores [15].

Existen otros ejemplos históricos de programas de recompensas, como el de Hunter & Ready, Inc. En 1983, esta empresa prometió un Volkswagen Beetle (popularmente apodado *Bug*) o un premio en efectivo de 1000 dólares a quien descubriera

errores en su sistema operativo VRTX (*Versatile Real-Time Executive*) [16]. Estas prácticas ya no son tan relevantes como un enfoque del *Bug-Bounty*, el cual sigue siendo apropiado en la actualidad y es bien visto por numerosas empresas para garantizar la seguridad de sus activos digitales y prevenir ataques y amenazas.

Sin embargo, en 1995 se lanzó lo que se considera el primer programa de *Bug-Bounty* en el sentido moderno, no como una táctica publicitaria o una apuesta divertida, sino como un esquema organizado y orientado a la seguridad de *software*, y con un sistema de recompensas monetarias. Con un fondo inicial de 50 000 dólares, los creadores del entonces popular navegador Netscape Navigator 2.0 establecieron un programa que otorgaba recompensas económicas, siendo el primero en utilizar el término *Bug-Bounty Program*, considerado por muchos el precursor de estos programas [17].

Crecimiento y consolidación

El ámbito de las recompensas por errores ha experimentado una expansión notoria desde la iniciativa de Netscape. Hoy se cuenta con más de un millón de participantes conocidos como "cazadores de errores", que persiguen recompensas financieras legítimas al hallar fallos en sistemas de grandes empresas. Plataformas de punta como *HackerOne*®, *Bugcrowd*® y *YesWeHack*® han integrado los programas de recompensas por errores y emplean técnicas de gamificación para motivar y retener a una gran comunidad de *hackers* éticos que realizan auditorías de seguridad para sus clientes, sin que exista una relación laboral formal entre las partes. [18]. Esta estrategia promueve una motivación constante y estimula la competencia entre los *hackers*, quienes buscan posicionarse en clasificaciones, ganar accesos a eventos prestigiosos o acumular puntos que incrementan su estatus en la comunidad y pueden intercambiarse por artículos promocionales de las respectivas compañías [19].

Tipos de *Bug-Bounty*

Por un lado, las empresas pueden establecer programas de recompensas por errores gestionando equipos dedicados a la recepción, comprobación y administración de las incidencias notificadas. Este proceso puede estructurarse mediante el uso de un correo electrónico específico o a través de sistemas diseñados para tal fin. Por otro lado, existen servicios especializados como *Intigriti*® y otros ya mencionados, que ofrecen un puente entre las empresas y una extensa red de auditores de seguridad, quienes están dispuestos a inspeccionar los activos digitales a cambio de una compensación [20].

Los esquemas de recompensas por vulnerabilidades pueden ser instaurados por la propia entidad o con la ayuda de una firma especializada en el área. Estos programas se clasifican en dos categorías principales: abiertos al público y de carácter privado.

- **Los programas públicos**: los esquemas de recompensas públicos están disponibles para todos y permiten que cualquier interesado pueda inscribirse y contribuir en ellos. Suelen ser implementados por organizaciones con una infraestructura amplia y un nivel avanzado en seguridad, las cuales poseen una multiplicidad de activos digitales y necesitan un volumen considerable de auditores que examinen su seguridad de forma continua [21].
- **Los programas privados**: son selectivos y solo permiten la participación de individuos cuidadosamente escogidos, los cuales son invitados directamente, seleccionados por su puntuación acumulada o después de pasar un proceso de verificación de identidad [22]. Estos programas son la opción predilecta para entidades que están incursionando en el ámbito de *Bug-Bounty* o para aquellas cuyos sistemas no pueden gestionar un alto número de auditorías simultáneas, sobre todo para las que priorizan la calidad frente a la cantidad. Esto les permite escoger detenidamente a los auditores que tendrán acceso a sus activos digitales.

Tanto los programas públicos como los privados pueden operar bajo el modelo de Programas de divulgación de vulnerabilidades (VDP por sus siglas en inglés), lo que significa que algunos programas de recompensas por errores no son monetarios, y que en lugar de dinero otorgan puntos canjeables dentro de las plataformas de recompensas por

errores, *merchandising* o beneficios propios de la empresa, como millas para viajeros frecuentes o productos como bebidas energéticas. No obstante, los programas más atractivos para los auditores son aquellos que ofrecen compensaciones económicas, como el pago en efectivo por cada vulnerabilidad de seguridad detectada y reportada [23].

Ventajas y desventajas de *Bug-Bounty*

Desventajas del *Bug-Bounty*

A pesar de que los programas de recompensas por hallazgos de errores están ganando mayor aceptación y muchas entidades podrían verse tentadas por su creciente popularidad, es crucial estar conscientes de los potenciales inconvenientes y desafíos que puede representar para una empresa la aceptación de una iniciativa de este tipo. A continuación, se enumeran y discuten en detalle cada una de estas desventajas que puede tener la implementación de un programa de *Bug-Bounty* [24].

- **Recibir masivamente reportes**: los programas de recompensa por errores a menudo generan una oleada de informes de seguridad provenientes de numerosos investigadores, entre los cuales puede haber una proporción significativa de baja calidad. Las empresas necesitan estar equipadas para procesar esta gran cantidad de informes, con personal capacitado para discernir entre los reportes valiosos y los que no lo son. Es esencial establecer directrices claras y específicas para el programa, para prevenir malentendidos y conflictos con los investigadores durante la selección de los informes [25].
- **Controlar a los cazadores de recompensas**: colaborar con una colectividad internacional de cazadores de errores podría implicar una falta de control sobre sus prácticas y técnicas empleadas en la búsqueda de fallos de seguridad. Este escenario puede complicar la administración efectiva del programa de recompensas y elevar la posibilidad de que datos delicados o confidenciales queden expuestos durante las investigaciones. Los investigadores poseen diversas motivaciones y podrían recurrir al uso de métodos o herramientas que amenacen la operatividad de los servicios inspeccionados, decidan explotar una vulnerabilidad para su propio interés o incluso lleguen a perjudicar la imagen de la empresa. Por ende, es crítico implementar estrategias de control rigurosas para atenuar estos riesgos.
- **Altos costos**: es esencial que las compañías realicen un análisis exhaustivo y fortalezcan la seguridad de su *software* o sus activos digitales antes de ofrecer recompensas económicas a terceros para descubrir fallos. En ausencia de una previa revisión de seguridad rigurosa, podría darse una situación en la que el volumen de vulnerabilidades identificadas por los auditores externos exceda el presupuesto destinado para las recompensas. Un caso notorio es el de *Shopify*®, que tuvo que pausar su programa de *Bug-Bounty* temporalmente, al tener que pagar una cantidad considerable —hasta 356 000 dólares diarios—, debido a la multitud de problemas de seguridad detectados en su *software*. Por tanto, validar y asegurar la robustez del *software* es un paso crítico antes de proceder con el lanzamiento de un programa de recompensas por errores [26].
- **Dificultad para encontrar auditores de calidad**: el mercado de la ciberseguridad, efectivamente, enfrenta el desafío de la escasez de talento calificado, lo cual se refleja en la dificultad para hallar auditores de alta calidad a participar en programas de *Bug-Bounty*. Los *bugs hunters* con amplia experiencia y un historial comprobado de descubrimientos significativos son altamente valorados en la industria; a menudo están comprometidos con empleos estables o proyectos de gran envergadura. Este factor limita la disponibilidad de profesionales capaces de dedicar tiempo considerable para comprender y examinar sistemas complejos que requieren un alto grado de pericia y atención al detalle [27].

Las organizaciones pueden afrontar este desafío fomentando relaciones a largo plazo con

auditores de confianza y utilizando plataformas de *Bug-Bounty* que permitan identificar y atraer talentos con las habilidades técnicas y analíticas deseadas. También pueden optar por programas de *Bug-Bounty* privados que faciliten la selección y colaboración con auditores que posean las competencias específicas para sus proyectos.

Ventajas del *Bug-Bounty*

En efecto, los programas de *Bug-Bounty* presentan varias ventajas significativas para las organizaciones, que incluyen: detectar errores de manera rápida y efectiva, proteger la información y los datos sensibles y establecer relaciones fortalecidas con la comunidad *hacker* [28]. En resumen, un programa de esta naturaleza puede ser una excelente manera de proteger una empresa y mejorar su seguridad informática. A continuación, se enumeran y discuten cada una de las ventajas que puede tener la implementación de un programa como este [29].

- **Sin limitantes**: trae ventajas significativas en términos de seguridad informática y de la gestión de vulnerabilidades [30].
- **Aprovechamiento de la comunidad de *hackers***: la colaboración con *hackers* éticos brinda a las empresas acceso a un grupo diverso de talentos y a sus habilidades, que pueden ser difíciles de encontrar y retener en el mercado laboral.
- **Mayor alcance de pruebas**: diversos individuos ofrecen diferentes métodos y perspectivas, lo que puede resultar en un conjunto más amplio de vulnerabilidades a descubrir, en comparación con los equipos de seguridad internos, que pueden tener un alcance limitado o seguir metodologías estándar.
- **Motivación por recompensas**: el modelo de recompensa no solo incentiva la participación, sino que también puede motivar a los participantes a encontrar vulnerabilidades críticas de forma más rápida y eficaz. Esto a menudo resulta en una detección más rápida de errores que podrían llevar más tiempo descubrir con métodos tradicionales.
- **Flexibilidad y escalabilidad**: permiten a las empresas escalar sus esfuerzos de seguridad conforme sea necesario, sin la necesidad de invertir en recursos internos adicionales.
- **Innovación continua**: los *hackers* suelen estar a la vanguardia de las técnicas de explotación y defensa, lo que significa que los programas de *Bug-Bounty* pueden permitir que las empresas se mantengan actualizadas sobre las nuevas tendencias y avances en el campo de la seguridad informática.

El éxito de estos programas de recompensas por errores depende de que la empresa pueda administrar de manera adecuada los informes de vulnerabilidades, mantener una comunicación clara y efectiva con los investigadores y procesar y solucionar rápidamente los problemas identificados. Además, es crucial que se establezcan reglas claras y precisas para garantizar que los *bugs hunters* actúen dentro de los límites éticos y legales durante sus investigaciones.

- **Costo-efectividad**: en un modelo tradicional de auditoría o *pentesting*, las empresas suelen pagar por el tiempo y los recursos, independientemente de los resultados. En cambio, los programas de *Bug-Bounty* requieren pago solo por los problemas de seguridad que sean correctamente encontrados y verificados, lo cual puede ser más económico para las empresas con muchos activos digitales.
- **Escalabilidad de recursos**: los programas de *Bug-Bounty* abren la puerta a un número potencialmente ilimitado de participantes, cada uno con sus propias habilidades y herramientas, lo que puede resultar en una cobertura de seguridad más amplia que la que podría proporcionar un equipo interno o una consultoría de seguridad con recursos limitados.
- **Eficiencia temporal**: mientras que los servicios de *pentesting* son generalmente periódicos y pueden dejar períodos de exposición entre las pruebas, los programas de *Bug-Bounty* funcionan continuamente y permiten la detección y corrección de vulnerabilidades de manera más ágil.

- **Pago por valor**: el pago basado en resultados también puede motivar a los *bugs hunters* a buscar vulnerabilidades más profundas y críticas, ya que estas a menudo ofrecen recompensas más altas, proporcionando así un mejor retorno de la inversión en términos de seguridad.

Sin embargo, para que un programa de *Bug-Bounty* sea efectivo, las organizaciones deben estar capacitadas para diligenciar el flujo de reportes y tener los recursos necesarios para validar y solucionar rápidamente las vulnerabilidades encontradas. Esto incluye tener un sistema robusto de triaje para separar los hallazgos críticos de los menos importantes y garantizar que solo se pague por reportes de alta calidad.

- **Imagen proyectada**: la gestión de la imagen y la reputación es crucial para cualquier empresa; los programas de *Bug-Bounty* pueden influir positivamente en este aspecto [31].
- **Compromiso con la seguridad**: la implementación de un programa de *Bug-Bounty* transmite un mensaje claro de que una empresa toma en serio la seguridad de sus datos e información tecnológica y la protección de los datos de los clientes.
- **Transparencia**: estos programas pueden ser vistos como una iniciativa transparente que muestra la disposición de la empresa a exponer sus vulnerabilidades para mejorar, en lugar de ocultarlas y correr el riesgo de que sean explotadas maliciosamente.
- **Colaboración con la comunidad de seguridad**: establecer relaciones con la comunidad de *hackers* éticos puede ayudar a construir una red de defensores externos y de expertos, y convertirse en recursos valiosos en el esfuerzo continuo por mejorar la seguridad.
- **Prevención frente a explotación**: cuando las vulnerabilidades se reportan y solucionan mediante estos programas, se reduce la probabilidad de que sean descubiertas y explotadas por atacantes, lo que podría causar daños más significativos, tanto operativos como a la imagen de la empresa.

Es importante que la empresa maneje con corrección su programa de *Bug-Bounty* y comunique de forma abierta cómo aborda y soluciona las vulnerabilidades encontradas. Una gestión deficiente o una mala comunicación podrían tener el efecto contrario y dañar la imagen pública de la organización. Por lo tanto, el lanzamiento y la gestión de estos programas deben realizarse de manera estratégica y profesional.

- **Reportes novedosos y de actualidad**: un programa de *Bug-Bounty* permite aproximaciones novedosas y relevantes al problema [32], y ayuda a las organizaciones en lo siguiente:
- **Identificar riesgos emergentes**: los *hackers* participantes a menudo buscan y prueban técnicas de explotación recientes y emergentes, lo que puede ayudar a descubrir riesgos que de otro modo podrían permanecer ocultos.
- **Actualizar continuamente las defensas de seguridad**: la retroalimentación continua de la comunidad permite que las defensas de seguridad de la organización se adapten y evolucionen como respuesta a las tendencias actuales de amenazas.
- **Promover una mentalidad proactiva**: con los reportes actualizados, la empresa puede cambiar de una postura reactiva a una más proactiva en seguridad, con la que busca y mitiga vulnerabilidades antes de que sean explotadas.
- **Mantener el ritmo con el panorama de amenazas dinámico**: la ciberseguridad es un campo que cambia con rapidez; mantenerse al día con las últimas vulnerabilidades y técnicas de explotación es fundamental. Los programas de *Bug-Bounty* son una forma de mantenerse actualizado con este ritmo acelerado.

El resultado es una postura de seguridad más robusta que puede adaptarse rápido a nuevos retos y disminuir el riesgo de una amenaza de seguridad, para proteger los activos digitales de la empresa, como su imagen y su reputación.

Ventajas y desventajas del *pentesting*

Desventajas del *pentesting*

Aunque los procesos de *pentesting* pueden ser útiles para encontrar fallos y errores en los sistemas de una organización, y mejorar su postura de seguridad, también presentan ciertas desventajas que es importante conocer. A continuación, se discutirán algunas de estas desventajas y también se enunciarán y analizarán en detalle cada una de ellas para comprender sus implicaciones [33].

- **Limitantes en tiempo y recursos**: el tiempo y el uso de recursos limitados en la aplicación de un *pentesting* pueden ser una desventaja, ya que limitan la capacidad del equipo de seguridad o de los evaluadores externos para realizar un examen exhaustivo y profundo del sistema o de una aplicación. Esto puede dificultar la identificación de todas las vulnerabilidades y debilidades existentes, lo que afecta la seguridad del sistema o la aplicación, y exponerlos a posibles ataques o amenazas [34].
- **Costos altos**: el *pentesting* puede ser un proceso costoso, debido a la necesidad de contratar evaluadores externos con conocimientos y habilidades especializadas en seguridad informática [35], así como de adquirir herramientas y tecnologías específicas para realizar la evaluación. Además, puede requerir una dedicación de tiempo y recursos por parte del equipo de seguridad de una organización, lo que podría generar costos indirectos en términos de salarios y cargas sociales.

Ventajas del *pentesting*

Los procesos de *pentesting* ayudan a una organización a identificar vulnerabilidades y mejorar su seguridad. Además, en algunos sectores regulados es un requisito para cumplir con estándares de seguridad. Por lo tanto, es importante conocer las ventajas de aplicar este tipo de procesos. Se enumeran a continuación sus ventajas [36]:

- **Profundidad y control**: permite detectar problemas de seguridad que podrían pasar desapercibidos por el equipo interno de seguridad de una organización. Definitivamente, el *pentesting* es una herramienta crucial para la prevención de ataques y amenazas, al mejorar la seguridad del sistema o aplicación evaluados [37].
- **Cumplimiento de estándares de seguridad**: en algunos sectores regulados, como la industria financiera o la salud, el *pentesting* puede ser un requisito para cumplir con estándares de seguridad [31]. Aplicarlo ayuda a una organización a cumplir con estos requisitos y a evitar sanciones o multas. Por lo tanto, es importante considerarlo como una medida de seguridad esencial en estos sectores.

Principales herramientas utilizadas en *pentesting* y *Bug-Bounty*

Herramientas del *pentesting*

El *pentesting* utiliza una variedad de herramientas especializadas para evaluar la seguridad. Entre las más destacadas se encuentran las siguientes [38]:

- ***Metasploit*:** se destaca como una plataforma versátil para el desarrollo y ejecución de *exploits*; permite la simulación de ataques y la explotación de vulnerabilidades en objetivos remotos.
- ***Wireshark*:** funge como un analizador de protocolos de red, posibilita la inspección del tráfico y detecta anomalías que podrían indicar la presencia de vulnerabilidades.
- ***Nmap*:** se emplea como un escáner de red, lo que facilita el descubrimiento de servicios y dispositivos en una red.
- ***Burp Suite*:** constituye una suite integral de herramientas para llevar a cabo pruebas en aplicaciones *web*, identificar vulnerabilidades y evaluar su impacto.

- ***Kali Linux*:** se presenta como una distribución de Linux preinstalada con una oferta amplia de herramientas de *pentesting* que facilitan la implementación de pruebas de manera eficiente y segura.

Herramientas de *Bug-Bounty*

Para realizar *Bug-Bounty* se cuenta con una amplia gama de herramientas especializadas [39]:

- **OWASP ZAP (Zed Attack Proxy)**: esta herramienta permite identificar vulnerabilidades en aplicaciones *web*.
- **Herramientas de automatización**: agilizan el proceso de búsqueda y explotación de vulnerabilidades, tales como sqlmap para la inyección SQL y xsstrike para la detección y explotación de Cross-Site Scripting (XSS).

Además, en *Bug-Bounty* a menudo se recurre a *scripts* personalizados, para automatizar tareas específicas o para escanear en busca de vulnerabilidades determinadas, así como a herramientas de inteligencia de amenazas, las cuales permiten obtener información sobre las últimas amenazas y vulnerabilidades. De igual forma, también se utilizan las herramientas ya mencionadas, como Metasploit, Nmap y Burp Suite.

Conclusiones

El *pentesting* y el *Bug-Bounty* son dos enfoques complementarios que pueden ayudar a mejorar la seguridad de una organización. El primero realiza una evaluación profunda y exhaustiva del sistema o aplicación evaluados, identifica todas las vulnerabilidades y debilidades existentes y proporciona un plan de acción para corregirlas. El segundo, como principio, involucra a una comunidad diversa de expertos en seguridad conocidos como *bug hunters* o cazadores de errores, que buscan vulnerabilidades en sistemas, aplicaciones o servicios digitales, y son remunerados por los problemas de seguridad que reportan.

En resumen, una organización madura en seguridad debería realizar un proceso de *pentesting* activo, antes de ponerlo a disposición de grupos de *pentesters* dedicados a programas de *Bug-Bounty*. De esta manera, se puede garantizar que el sistema o aplicación evaluados estén lo más seguro posible, antes de someterse a la investigación y pruebas de los *hackers* externos. Además, al involucrar a los *hackers* externos en la búsqueda de vulnerabilidades con un programa de *Bug-Bounty*, se puede aprovechar su amplia gama de habilidades y conocimientos para identificar problemas que podrían pasar desapercibidos para los expertos internos de la organización; de este modo se puede optimizar el proceso de identificación de vulnerabilidades y mejorar la seguridad del sistema o aplicación evaluados.

El *pentesting* y el *Bug-Bounty* son enfoques complementarios para mejorar la seguridad de una organización. El primero implica una evaluación profunda y exhaustiva del sistema o aplicación, mientras que el segundo involucra una comunidad global de *hackers* éticos para identificar vulnerabilidades en sistemas y aplicaciones. La implementación de ambos enfoques, junto con medidas preventivas y correctivas, puede ayudar a proteger a una organización contra amenazas y ataques externos.

Referencias

[1] S. Shah y B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques", *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 27-49, 2014.

[2] U. Ravindran y R. V. Potukuchi, "A review on Web application vulnerability assessment and penetration testing", *Review of Computer Engineering Studies,* vol. 9, no. 1, pp. 1-22, 2022.

[3] L. Irwin, "Top 5 cyber security risks for businesses," *IT Governance UK Blog*, 19 de jul. de 2022, [en línea], disponible en: https://www.itgovernance.co.uk/blog/top-5-cyber-security-risks-for-businesses. [Consultado: 19-Nov-2022].

[4] Colombia Digital, *5 amenazas de ciberseguridad que en 2022 atacarán en Colombia*, Corporación Colombia Digital, 26-ene-2022, [en línea], disponible en: https://colombiadigital.net/opinion/5-amenazas-de-ciberseguridad-que-en-2022-atacaran-en-colombia. [Consultado: 19-Nov-2022].

[5] A. Mohan y D. G. Swaminathan, "Analysis of vulnerability assessment with penetration testing", *SSRN Electronic Journal*, 2022.

[6] S. Basu, "Difference between vulnerability assessment and penetration testing", *Astra Security Blog*, 28-mar-2022, [en línea], disponible en: https://www.getastra.com/blog/security-audit/vulnerability-assessment-vs-penetration-testing/. [Consultado: 20-Nov-2022].

[7] M. Finifter, D. Akhawe y D. Wagner, "An Empirical Study of Vulnerability Rewards Programs", in *22nd USENIX Security Symposium (USENIX Security 13)*, Washington DC, USA, pp. 273-288, 2013.

[8] D. R. McKinnel, T. Dargahi, A. Dehghantanha y K. K. R. Choo, "A systematic literature review and meta-analysis on artificial intelligence in penetration testing and Vulnerability Assessment", *Computers & Electrical Engineering*, vol. 75, pp. 175-188, 2019.

[9] T. Wilhelm, *Professional penetration testing creating and learning in a hacking lab*, 2nd ed. Amsterdam: Syngress, an imprint of Elsevier, 2013.

[10] L. Allen y K. Cardwell, *Advanced penetration testing for highly secured environments: Employ the most advanced Pentesting techniques and tools to build highly secured systems and environments*. Birmingham, UK: Packt Publishing, 2016.

[11] I. Soria-Guzmán (Ed.), F. Briones-Medina, E. Cabañes-Martínez, A. Miranda-Díaz, J.M. Serralde-Ruiz y G. Wolf-Izsaevich, *Ética hacker, seguridad y vigilancia*. CDMX: Universidad del Claustro de Sor Juana, 2016.

[12] M. G. Jaatun, D. S. Cruzes, K. Bernsmed, I. A. Tøndel y L. Røstad, "Software security maturity in public organisations", *Lecture Notes in Computer Science*, pp. 120-138, 2015.

[13] H. Fryer y E. Simperl, "Web science challenges in researching Bug Bounties," in: *Proceedings of the 2017 ACM on Web Science Conference*, Troy, New York, USA, 2017.

[14] S. Ditlea, "Rewriting the Bible in 0's and 1's", *Technology review*, vol. 102, no. 5, pp. 66-70, 1999.

[15] Google, "Hacking Google, Episode 4, Bug-Bounty", YouTube, 3-oct-2022, [en línea], disponible en: https://www.youtube.com/watch?v=IoXiXlCNoXg [Consultado: 27-Nov-2022].

[16] Hunter & Ready Inc., "VRTX poster, catalog number 102782474", *Computer History Museum, 1983*, [en línea], disponible en: https://www.computerhistory.org/collections/catalog/102782474 [Consultado: 29-Nov-2022].

[17] J. Wachs, "Making markets for information security: the role of online platforms in Bug-Bounty programs", *arXiv preprint arXiv:2204*. 06905, 2022.

[18] J. O'Hare y L. A. Shepherd, "Proposal of a Novel Bug-Bounty Implementation Using Gamification", *arXiv preprint arXiv:2009*. 10158, 2020.

[19] A. Laszka, M. Zhao, A. Malbari y J. Grossklags, "The rules of Engagement for Bug-Bounty programs", *Financial Cryptography and Data Security*, pp. 138-159, 2018.

[20] P. García-Pérez, *Bug-Bounty: de profesión "cazarrecompensas"*. Móstoles, Madrid: ZeroxWord Computing, 2021.

[21] O. Espino, "Bug-Bounty Collection: More than $$$$$ USD in rewards by legally hacking big companies". *Independiente*, 2022.

[22] J. Restrepo, "Lo que nadie te dijo antes de dedicarte al Bug-Bounty", *HackTheBox & RedTeamRD. 2020*, [en línea], disponible en: https://www.youtube.com/watch?v=4SwV1TnkwJA [Consultado: 29-Nov-2022].

[23] A. Laszka, M. Zhao y J. Grossklags, "Banishing misaligned incentives for validating reports in bug-bounty platforms", *Computer Security - ESORICS 2016*, Heraklion, Creta, Grecia, pp. 161-178, 2016.

[24] T. Walshe y A. C. Simpson, "Coordinated vulnerability disclosure programmer effectiveness: Issues and recommendations", *Computers & Security*, vol. 123, p. 102936, 2022. https://doi.org/10.1016/j.cose.2022.102936.

[25] H. Hata, M. Guo y M. A. Babar, "Understanding the Heterogeneity of Contributors in Bug-Bounty Programs", in *Proceedings of the 11th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, Toronto, Ontario, Canada, pp. 223-228, 2017.

[26] J. Peñalba, "The Worst Bug-Bounty Ever", Rooted CON, 22-Ago-2017, [en línea], disponible en: https://www.youtube.com/watch?v=pf1TZn1YnXA [Consultado: 29-Nov-2022].

[27] HackerOne, "The 2020 Hacker Report", [en línea], 2020, disponible en: https://www.hackerone.com/sites/default/files/2020-04/the-2020-hacker-report.pdf [Consultado: 03-Dic-2022].

[28] O. Akgul *et al.*, "Bug hunters' perspectives on the challenges and benefits of the Bug-Bounty", in: *32nd USENIX Security Symposium (USENIX Security)*, Anaheim, California, USA, vol. 2301, 2023. https://doi.org/10.48550/arXiv.2301.04781.

[29] S. Atefi, A. Sivagnanam, A. Ayman, J. Grossklags y A. Laszka, "The benefits of Vulnerability Discovery and

Bug-Bounty programs: Case studies of chromium and firefox", in: *Proceedings of the ACM Web Conference 2023*, Austin, Texas, USA, 2023. https://doi.org/10.1145/3543507.3583352.

[30] A. Kuehn y M. Mueller, "Analyzing Bug-Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities", *TPRC Conference Paper*, disponible en: https://ssrn.com/abstract=2418812, 2014.

[31] O. Akgul, T. Eghtesad, A. Elazari, O. Gnawali, J. Grossklags, M. L. Mazurek, D. Votipka y A. Laszka, "Proposal of a Novel Bug-Bounty Implementation Using Gamification", *arXiv preprint arXiv:2301.04781*, 2023.

[32] L. Breidenbach, P. Daian, F. Tramèr y A. Juels, "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts", in: *27th USENIX Security Symposium (USENIX Security 18*), Baltimore, Maryland, USA, pp. 1335-1352, 2018.

[33] F. M. Teichmann y S. R. Boticiu, "An overview of the benefits, challenges, and legal aspects of penetration testing and red teaming", *International Cybersecurity Law Review*, 2023. https://doi.org/10.1365/s43439-023-00100-2.

[34] R. Böhme y M. Félegyházi, "Optimal Information Security Investment with penetration testing", *Lecture Notes in Computer Science*, pp. 21-37, 2010.

[35] Cobalt, "The State of Pentesting 2022", 2022, [en línea], disponible en: https://www.cobalt.io/hubfs/State_of_Pentesting_2022.pdf. [Consultado: 07-Mar-2023].

[36] A. Aibekova y V. Selvarajah, "Offensive security: Study on penetration testing attacks, methods, and their types", *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, Ballari, Karnataka, India, 2022. https://doi.org/10.1109/icdcece53908.2022.9792772.

[37] M. Styles y T. Tryfonas, "Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users", *Information Management & Computer Security*, vol. 17, no. 1, pp. 44-52, 2009.

[38] S. Raj y N. K. Walia, "A study on Metasploit Framework: A pen-testing tool", *2020 International Conference on Computational Performance Evaluation (ComPE)*, Jul. 2020. https://doi.org/10.1109/compe49325.2020.9200028.

[39] S. S. Malladi y H. C. Subramanian, "Bug-Bounty programs for cybersecurity: Practices, issues, and recommendations", *IEEE Software*, vol. 37, no. 1, pp. 31-39, Jan. 2020. https://doi.org/10.1109/ms.2018.2880508.