Cuaderno Activa
Revista científica de la Facultad de Ingeniería

Detección y mitigación de vulnerabilidades día cero.

Mitigation and Detection of Zero-Day Vulnerabilities.

Juan Sebastián Guisao*
Juan Carlos Toro Rendón**

Tipo de artículo: Reflexión.

Recibido: 31 de agosto, 2014
Aceptado: 24 de octubre, 2014

Resumen

En el presente artículo se define el estado general de la seguridad informática con un enfoque hacia las vulnerabilidades día cero, y como estas comprometen a las organizaciones y los sistemas informáticos al estar expuestos a ataques que no se pueden controlar con herramientas conocidas, dado que se desconoce su solución. Dichos ataques se denominan ataques día cero. Con esta motivación se desea dar a conocer los mecanismos de gestión y mitigación de dichas amenazas por medio de una metodología de revisión de investigaciones, experiencias y modelos de gestión de detección rápida, con el fin de dar respuesta a: ¿Cuál es la evolución de la seguridad informática en la actualidad? ¿Qué es una vulnerabilidad día cero y qué papel juega en la rutina diaria de un administrador de seguridad? ¿Cuáles son los principales métodos de gestión de las vulnerabilidades y ataques día cero? Se efectúa una búsqueda en los principales medios digitales como: bases de datos indexadas, revistas y artículos, con el fin de clasificar la información relacionada con el tema de investigación, según los enunciados en el resumen, título o cuerpo de documentos publicados entre los años 2000 y 2014.

Palabras claves: vulnerabilidad día cero, ataque día cero, seguridad de la información, amenazas informáticas, gestión de amenazas informáticas.

Abstract

In this article the general state of information security focused on the zero-day vulnerability is defined and how are you committed to the organizations and systems to be exposed to attacks that can not be controlled with familiar tools since the solution is unknown. Such attacks are known as zero-day attacks, it is for this reason that you want to publicize the mechanisms for managing and mitigating these threats through a methodology review of research, experience and management models for early detection in order to to answer : What is the evolution of computer security today? what is a zero-day vulnerability and what role this plays in the daily routine of a security manager? What are the main methods for managing vulnerabilities and zero-day attacks? A search is performed on the main digital media as indexed databases, journals and articles , in order to classify the information related to the research topic as set out in the summary , title or body of the document made since 2000 to the year 2014 .

Keywords: zero-day vulnerability, zero day attacks , information security , cyber threats, management of IT threats.

* Ingeniero de Sistemas. Estudiante Especialización Seguridad de la Información. Representante de Servicios, Softnet S.A. sguisa@gmail.com

** Ingeniero de Sistemas. Estudiante Especialización Seguridad de la Información. Representante de Servicios, Softnet S.A. jct_86@hotmail.com

Introducción

El aumento constante en el uso de la tecnología informática, conlleva también al crecimiento de los ataques y amenazas que se presentan contra la información manejada. Es por esto que es importante mantener un control y una medición permanentes del estado del sistema contra vulnerabilidades existentes, y conocer qué tan preparado se está para reaccionar frente a un posible ataque.

De igual manera, es a hoy una realidad que las empresas requieren para procesar su información de herramientas informáticas, las cuales se pueden ver expuestas a fallas de desarrollo de software y bugs de compatibilidad con los entornos, además de otros factores que requieren un constante proceso de análisis para que puedan mitigar los efectos de ataques desconocidos o no previstos llamados ataques día cero.

En el presente documento se hace un análisis reflexivo acerca de cómo detectar vulnerabilidades y cómo reducir el impacto ocasionado por la aparición de nuevas amenazas en cada sistema, incluyendo el uso de herramientas como anzuelos o honeypots, que desvían la atención de posibles atacantes.

Marco teórico

Las infraestructuras empresariales incrementan su confianza en sistemas de cómputo conectados a la red, por lo tanto se hace necesario asegurar estos sistemas contra posibles intrusiones. Emprender el mejoramiento de la seguridad en la red corporativa parte del análisis y medición de la misma, dado que solo es susceptible de ser mejorado aquello que puede ser medido. Una métrica de la seguridad de la red es deseable y con ella se podrá comparar el antes y el después de aplicadas las herramientas de seguridad (Wang et al., 2010).

Hoy en día los ataques de seguridad son más insidiosos de lo que solían ser. Usan una combinación de técnicas mixtas y están orientados a la consecución de un resultado o de un objetivo en específico, como el robo de información con fines económicos. El término APT (amenaza persistente avanzada, por sus siglas en inglés) describe las características de ataques que usan múltiples enfoques para acceder a los sistemas, incluyendo ingeniería social, malware día cero y troyanos, los cuales comprometen la infraestructura informática empresarial y/o buscan formas de evadir los mecanismos de escaneo y detección para que puedan ser utilizados a largo plazo, pretendiendo generar así una ganancia financiera (Tankard, 2014).

Aunque el número de vulnerabilidades de seguridad crece todos los días, no se puede decir lo mismo sobre los métodos de defensa existentes, por lo cual el problema más delicado está en detectar ataques desconocidos, llamados ataques de día cero (Musca et al., 2013).

A pesar de esto, la divulgación de vulnerabilidades es una situación delicada; en muchos casos, las empresas afectadas prefieren notificar a sus proveedores o fabricantes de soluciones informáticas una vez son descubiertas estas vulnerabilidades, y trabajar con ellos para su mitigación en un periodo de tiempo. Otros creen que una vez descubierta la vulnerabilidad es muy probable que otras personas malintencionadas la aprovechen y busquen revelarla al público masivo tan pronto como sea posible (Potter, 2005)

Metodología para la detección de vulnerabilidades de redes de datos

Consta de tres fases soportadas por herramientas de software para vulnerabilidades en equipos conectados, tanto por medio cableado como inalámbrico; en cada fase se puntualizan las acciones que se deben realizar y cómo se deben llevar a cabo a través de las herramientas apropiadas.

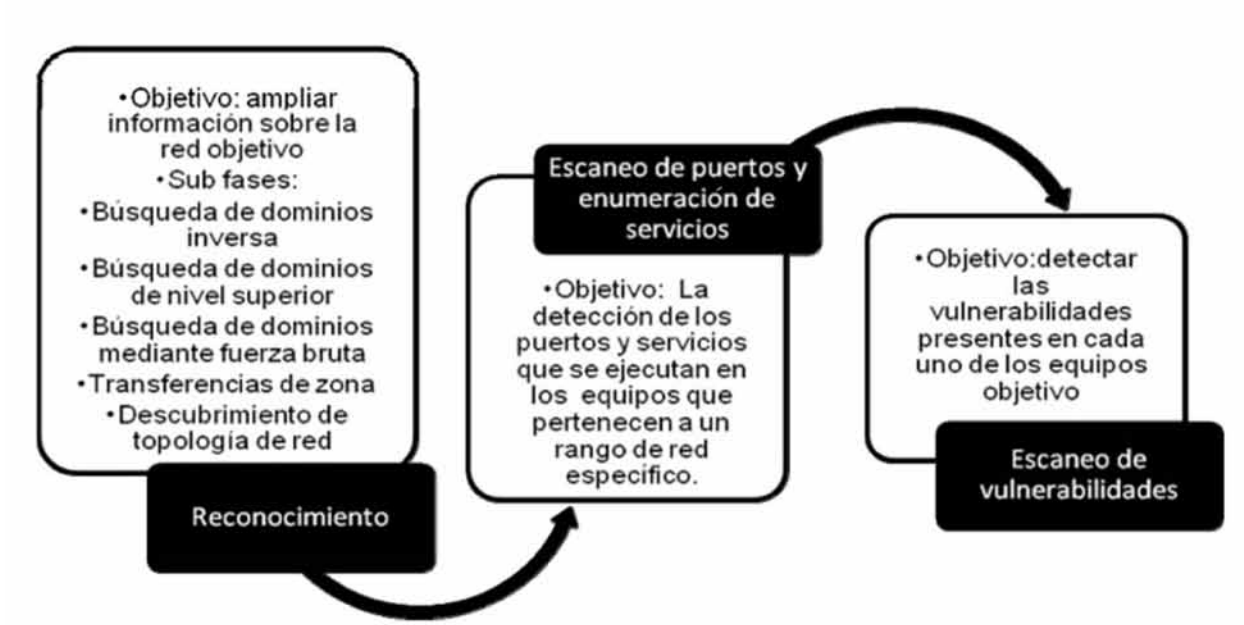


Figura 1. Esquema de la metodología de la detección de vulnerabilidades en redes de datos
Fuente: Franco et al. (2012)

La fases son descritas de la siguiente manera: la primera fase consiste en obtener información de la red objetivo, para lo cual se utilizan técnicas basadas en diferentes tipos de consultas a servidor DNS y análisis de los mensajes de enrutamiento; la segunda fase consiste en el escaneo y enumeración de los puertos y servicios activos con los que cuentan los equipos de cómputo obtenidos, a partir de esta información se puede conocer el rol que jugará cada equipo dentro de la organización y determinar así la criticidad del mismo dentro de la red objetivo; la fase final consiste en evaluar los equipos críticos para ir en búsqueda de vulnerabilidades, según lo encontrado en las fases anteriores (Franco et al., 2012).

Detección y análisis de vulnerabilidades día cero mediante el uso de anzuelos

A continuación, en la Figura 2 se nombra una metodología para la detección de ataques día cero, la cual consiste en combinar las ventajas de un anzuelo sombra (shadow-honeypot) y una detección de sistemas anómalos, con el fin de prevenir peticiones maliciosas y proteger las aplicaciones.

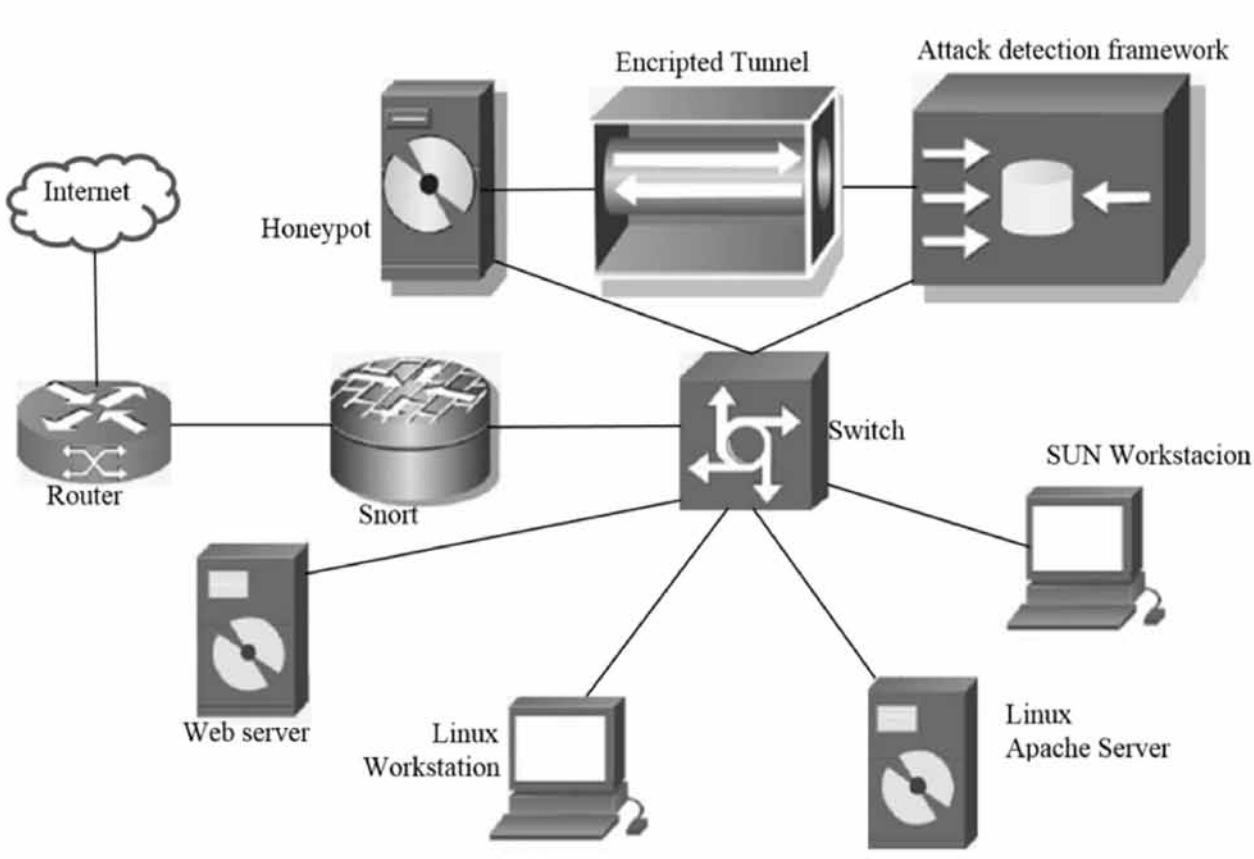


Figura 2. Arquitectura de sistema de detección
Fuente: Musca et al. (2013)

Con el fin de atraer a los atacantes, lo primero que se debe establecer es el anzuelo (honeypot) o anzuelos, los cuales tendrán que ser ubicados en la red junto a otros sistemas, como estaciones con diferentes sistemas operativos, servidores y otros. La red estará protegida por sistemas IPS e IDS que tendrán una configuración personalizada (en la imagen se nombran como "Snort"). Adicionalmente, se cuenta con un honeypot que se comunica a través de un canal cifrado a una máquina protegida donde estará corriendo el marco de detección de ataques (Attack Detection Framework); de esta manera se podrá mantener un control y visualización de las amenazas que se están presentando en la red y filtrarlas (Musca et al., 2013).

Mitigación

- Hay que asegurarse de tener un buen cortafuegos, configurado para permitir solo el tráfico mínimo necesario.
- El corta fuegos es fundamental a la hora de proteger el sistema contra amenazas de día cero. Configurándolo de forma adecuada, solo permitirá las transacciones absolutamente necesarias.
- Cuantos más programas tenga un sistema, más vulnerable será. Utilizando únicamente las aplicaciones esenciales, el riesgo para la red será menor.
- Mantenga actualizados los parches de los proveedores de los programas.

- Los parches corrigen vulnerabilidades del software y de los sistemas operativos, haciéndolos más resistentes ante los programas maliciosos.
- Utilice un sistema de prevención contra intrusiones (NIPS) para detener cualquier otra amenaza.

El análisis de comportamiento es un método habitual de los sistemas de prevención contra intrusiones. El código y los programas desconocidos pueden ejecutarse, pero se vigilan para identificar comportamientos maliciosos. Sin embargo, se pueden producir daños durante la ejecución de la amenaza (Corporation, s.f.).

Conclusiones

Se logra evidenciar en el presente artículo cómo a partir de la identificación aislada de las vulnerabilidades ante un ataque, es posible medir las acciones de defensa que se pueden establecer dentro de la red afectada.

A pesar de que las vulnerabilidades día cero estén en aumento, aún se observa que falta mucho crecimiento para que la protección se ajuste a la curva exponencial que presentan las amenazas. Asimismo, vale la pena que la protección no solamente sea reactiva, sino que genere un mecanismo proactivo con una correcta personalización de los sistemas IPS e IDS.

Es necesario garantizar que en el interior de las organizaciones se cuente con procedimientos de mitigación y revisión de puertos y servicios habilitados, con el fin de tomar acciones como actualizaciones, mejores prácticas o configuraciones seguras de los distintos servicios que sean de misión crítica.

Debido a la gran cantidad de ataques, amenazas y vulnerabilidades que afronta día a día cada organización, es válido el uso de granjas de servidores y equipos como engaño (honeypots) que presenten vulnerabilidades manejables para validar cada ataque y estar al tanto de las acciones desplegadas; de esta manera los ataques no se concretan en los servidores principales.

La detección temprana de vulnerabilidades día cero le permite a las organizaciones tomar acciones de divulgación, informando a entidades y fabricantes, lo cual permitiría contar con tiempos de respuesta rápidos y con acciones que favorezcan a otros posibles afectados; así se evita el daño en los servicios y se mitiga el impacto.

Referencias

Corporation, S. (s.f.). *Sophos Corporation*. Recuperado de http://www.sophos.com/es-es/security-news-trends/security-trends/zeroday-threats.aspx

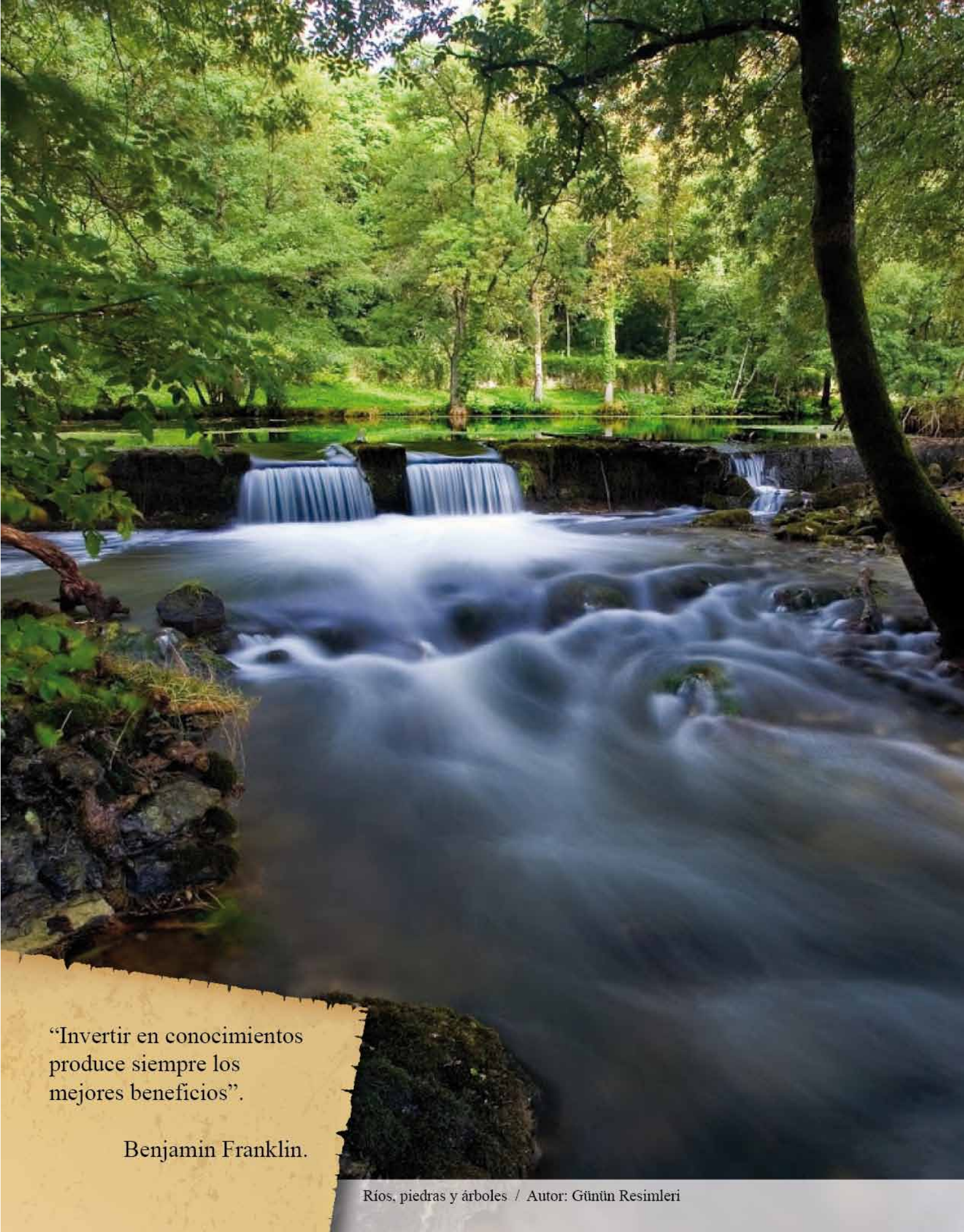
Franco, D., Perea, J., & Puello, P. (2012). Metodología para la detección de vulnerabilidades en redes de datos. *Información Tecnológica*, 113-120.

Musca, C., Mirica, E., & Deaconescu, R. (2013). *Detecting and Analyzing Zero-Day Attacks Using Honeypots. Proceedings* - 19th International Conference on Control Systems and Computer Science, 543-548.

Potter, B. (2005). The End of Zero Days? *Network Security*, (10), 10-11.

Tankard, C. (2014). New Rules for Combat New Threats. *Computer Fraud and Security*, 4, 14-16.

Wang, L., Jajodia, S., Singhal, A., & Noel, S. (2010). *K-zero Day Safety: Measuring the Security Risk of Networks Against Unknown Attacks*. Computer Security, ESORICS 2010 - 15th European Symposium on Research in Computer Security, Proceedings, 573-587.



"Invertir en conocimientos produce siempre los mejores beneficios".

Benjamin Franklin.

Ríos, piedras y árboles / Autor: Günün Resimleri