Honeypots dinámicos basados en Blockchain

Danitza Helen Vallejos Quiñones
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
helen.vallejos.q@gmail.com

***Resumen*—Los Honeypots proporcionan al atacante todos los recursos necesarios para que un ataque sea exitoso, lo que permite a la organización un estudio de las técnicas y procedimientos que realizó el hacker, para su documentación y aprendizaje para futuros incidentes. Sin embargo, en los Honeypots tradicionales, el atacante puede identificarlos fácilmente, el uso de los Honeypots dinámicos pueden pasar desapercibidos, por la semejanza con un servicio real. El uso de la tecnología Blockchain ayudará la descentralización del sistema y almacenar los datos mediante una cadena privada.**

Palabras clave—Blockchain, Honeypots, host, red, P2P.

I. INTRODUCCIÓN

Un Honeypot, es un software o conjunto de elementos de red, cuya intención es atraer atacantes, simulando ser un sistema vulnerable a los ataques, los honeypots se ha convertido en una herramienta indispensable para proporcionar seguridad, a varias aplicaciones con ser el Internet de las cosas (IoT). Además de ser una fuente para obtener información sobre las técnicas utilizadas en los ataques de las redes de comunicación [1].

Esta herramienta está diseñada especialmente para servir como una trampa contra posibles ataques, tienen la capacidad de simular un servicio o dispositivo con el objetivo de atraer acciones, que posteriormente son analizadas [2].

Los Honeypots se pueden clasificar en dos categorías, los estáticos están diseñados para engañar a los atacantes imitando alguna de las características del sistema. Sin embargo, debido a la configuración fija, estas son propensas a ser detectados por los atacantes. Mientras que los honeypots dinámicos mejoran la debilidad de los estáticos, debido a su configuración cambiante, es decir que es capaz de engañar a los intrusos y aprender de los nodos de ataque [2].

Uno de los mayores desafíos al implementar cualquier tipo de sistema de seguridad es mantener la funcionalidad del sistema a medida que este cambie, por lo que se ha convertido en un problema común en los honeypots, ya que se debe lograr que se entremezclen entre los sistemas verdaderos y estos pasen desapercibidos.

Un honeypot dinámico, debería ser capaz de funcionar sin la necesidad de actualizarlo constantemente, además de identificar las ip, que no pertenecen al sistema de manera automática [2].

Blockchain es una red descentralizada, conocida como cadena de bloques, se caracteriza porque la información recogida está distribuida en varios ordenadores, denominados nodos, donde se almacenan copias que se actualizan en tiempo real entre todos los nodos, que tienen la misma importancia. El esquema descentralizado de la tecnología Blockchain, ayudará a que la herramienta honeypot mantenga un funcionamiento normal, por lo que no importa si un host central se bloquee en el sistema.

A. Blockchain.

La cadena de bloques es una base de datos que puede ser compartida por una gran cantidad de usuarios de forma peer-to-peer, que permite almacenar información de forma inmutable y ordenada.

Las bases de datos o registros de información centralizados, se pueden definir como aquellos en las que los datos se almacenan en un lugar físico, un único servidor, aunque este sea accesible desde otros lugares. Blockchain nace como una propuesta de registros de información distribuido y opera de manera que cada una de las computadoras o servidores conectados a la base de datos tienen una copia de todo el sistema Blockchain.

P2P hace referencia a la interacción entre los distintos participantes que se denominan nodos, estos nodos están conectados entre sí, cuando un nodo quiere informar al resto de nodos de una transacción, le envía la información sobre la misma a aquellos con las que está conectado y estos la replican con aquellos, que a su vez estaban conectados este proceso se itera hasta que la información este compartida por toda la red.

Funcionamiento de la tecnología Blockchain: los procesos mediante el cual se genera la información y se publican nuevos bloques validos pueden describirse en los siguientes pasos:

El primer paso consiste en enviar la información en forma de transacciones que finalmente acabarían constituyendo los bloques de la misma, es decir cuando un nodo quiere realizar una transacción, le envía la información sobre esa transacción a los nodos con los que está conectado.

En el segundo paso, cada nodo va llevando su pool con las transacciones que va escuchando. En general, los pools de dos nodos diferentes no tienen por qué coincidir puesto que lo normal es que escuchan las transacciones en distinto orden.

El tercer paso, cada ronda dependiendo del Blockchain tienen lugar tras un tiempo que puede variar, en promedio desde unos pocos segundos hasta varios minutos en, un nodo que es escogido aleatoriamente para proponer un bloque. Este proceso es el más importante, haciendo que Blockchain sea una base de datos donde distintas partes no tienen por qué confiar unas en otras.

Para referenciar este artículo (IEEE):

[N] D. Vallejos, «Honeypots dinámicos basados en Blockchain», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 65-67, 2020.

En el cuarto paso, la persona elegida propone un bloque nuevo con las transacciones que ha ido "escuchando" y registrando su pool. Antes de ser enviado a los demás nodos, este nodo es validado por un hash, que es el código alfanumérico obtenido a partir de toda la información del bloque [3].

B. Honeypots.

Un honeypot es un sistema diseñado para analizar como los atacantes emplean sus habilidades para intentar entrar a un sistema, alterar o destruir sus datos. Son servidores de información falsos, posicionados estratégicamente en una red de prueba, las cuales son alimentados con información inexistente que es disfrazada con información de naturaleza confidencial.

A su vez estos servidores son configurados de manera que sea complicado, pero no imposible ser vulnerados por un atacante, exponiéndolos de manera deliberada a posibles ataques [5].

Entre las funciones de un honeypot está:

- Desviar la atención del atacante de la red real, de manera que no se comprometan las aplicaciones principales.
- Capturar virus o gusano para su posterior estudio.
- Formar perfiles de atacantes y sus métodos de ataque, para construir un archivo del modus operandi de un atacante.
- Conocer las nuevas vulnerabilidades y riesgos de los distintos tipos de sistemas operativos, entornos y programas que aún no se encuentran documentadas.

Honeypots dinámicos. El servidor honeypot dinámico, comienza recopilando información sobre los hosts disponibles utilizando un enfoque activo o pasivo. El administrador tiene la opción de seleccionar el mejor enfoque de recopilación de datos, que se utilizará en función de la arquitectura de la red.

Si la red se compone de ordenadores conectados a través de un concentrador donde es factible el rastreo del paquete, el administrador puede ejecutar el servidor honeypot dinámico en modo pasivo, evitando la necesidad de generar paquetes de sondeo en el medio compartido.

Por otro lado, si la red consiste en una red conmutada donde los hosts se conectan al interruptor de la capa dos, la toma de huellas pasivas no sería tan confiable como en el sondeo activo, después de obtener la imagen completa de la red, incluidos los sistemas operativos y los servicios de los hosts en ejecución. El servidor honeypot dinámico estima la naturaleza y servicios de los sistemas falsos que se implementan, luego emite los parámetros de configuración adecuados para implementar los sistemas en la red.

La red tendría sistemas reales y falsos corriendo juntos, el intruso puede ser detectado usando las conexiones que se hacen en los sistemas inexistentes que son sistemas de producción que se supone que no perciben tráfico de la red, cualquier intento de interactuar con el sistema falso seria redirigido a un honeypot físico, que permite al hacker un mayor nivel de interacción [3].

II. MÉTODOS

Para el presente estudio se aplicaron los siguientes métodos y técnicas de investigación:

TABLA I. METODOLOGÍAS

Método	Honeypots	Blockchain
Deducción	Investigación a partir de un conjunto dado de premisas, dicho de otra forma, un modo de pensamiento que va de lo general a lo específico.	
Analítico	Es un método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos.	
Sintético		Es un proceso que tiende a reconstruir un todo, a partir de los elementos
Técnicas de investigación		
Investigación documental	Para el presente estudio, se usó la investigación documental, la cual fundamenta la recopilación de información, a partir de documentos y artículos relacionados con seguridad, Honeypots y Blockchain, provenientes de diferentes autores. Este estudio se realizó a partir de los conocimientos y teorías obtenidas de diferentes autores.	

Fuente: Elaboración propia

III. RESULTADOS

La plataforma Blockchain sirve como la capa inferior en el sistema, los hosts constituyen una cadena de bloques privadas que forman una red P2P, al calcular el valor hash del bloque, el host en la cadena privada puede extraer el bloque principal y subirlo a la cadena, este mecanismo garantiza que la arquitectura de despliegue, se distribuya y descentralice. El host temporal y principal ejecutará el algoritmo de asignación de servicios y enviará la información cifrada a otros hosts, es decir el host que calcule con éxito un hash en particular, se convierte en un host principal, como se muestra en la siguiente imagen.

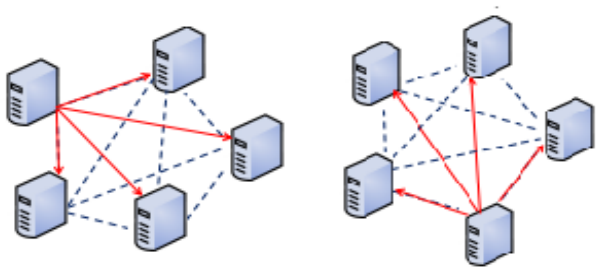

Fig. 1. Anfitriones principales
Fuente: Elaboración propia

Si el host configurado sufre de ataques y su rendimiento disminuye, no puede servir como el host contador por carecer de suficientes recursos informáticos, y otros hosts los reemplazarán automáticamente. Por lo tanto, la ruptura del host principal no hace diferencia en el sistema, es decir el sistema funciona normalmente.

Los ataques capturados por un host se cargan en Blockchain y otros nodos sincronizan estos registros en la cadena privada, por lo tanto, cada nodo tiene datos completos que se almacenan de manera segura y resistente a manipulaciones para futuros análisis forenses.

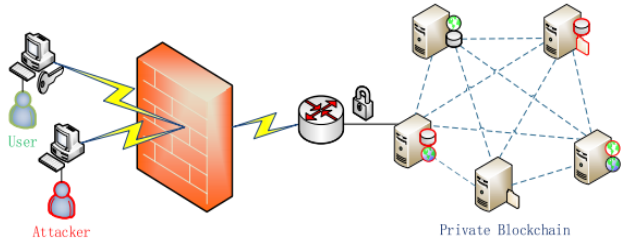

Fig. 2. Sistema honeypot distribuido dinámicamente
Fuente: Jia, Baoying, Honglong, Leyi, S., & Yang, L. Dynamic Distributed Honeypot based on Blockchain

El host del centro genera información de conversación que se asigna a cada host para iniciar diferentes servicios, es decir para iniciar un servicio real o honeypot.

Desde la perspectiva de seguridad, cada host puede ejecutarse en un modo normal o modo compromiso. Un modo normal indica que un host funcional sin datos maliciosos y mantiene su funcionamiento normal. Sin embargo, un modo de compromiso indica que el host se ejecuta de forma maliciosa y se daña a sí mismo [2].

IV. Conclusiones

El problema en una arquitectura distribuida, conduce a un problema, donde los datos almacenados en las bases de datos son alterables. Mientras en un esquema descentralizado basado en Blockchain, las bases de datos son inalterables, la información dinámica de estos esquemas se refleja en la implementación o configuración.

Sin embargo, la información solo es de los honeypots, en lugar del sistema real. Una vez que se reconoce estos honeypots, el sistema real se enfrenta a amenazas, mientras el esquema descrito anteriormente contiene tanto servicios reales como honeypots y al cambiar periódicamente los servicios reales, un atacante no puede encontrarlos, protegiendo así el sistema real.

Referencias

[1] Incibe-cert. (23 de marzo de 2017). Centro de respuesta a incidentes de seguridad. Obtenido de https://www.incibe-cert.es/

[2] Jia, L., Baoying, S., Honglong, C., Leyi, S., & Yang, L. (2019). Dynamic Distributed Honeypot based on Blockchain. IEEE.

[3] Kuwatly, I., Sraj, M., & Al Masri, Z. (2019). A dynamic Honeypot design for Intrusion Detection. IEEE.

[4] López, M. A. (2018). Blockchain, Como desarrollar confianza en entornos complejos para generar valor de impacto social. BID Banco Interamericano de Desarrollo.

[5] Mora, P. (2018). Honeypots. México.

Breve CV de la autora

Danitza Helen Vallejos Quiñones es Ingeniera de Sistemas por la Escuela Militar de Ingeniería (La Paz, 2015), diplomada en Gestión de incidentes de tecnología de la información, en la Escuela de Gestión Pública (La Paz, 2017).
Realizó un curso de E|SRI Seguridad y Respuesta ante Incidentes Informáticos en Hacking Bolivia (La Paz, 2019)
Ejerce actualmente como Operadora de Infraestructura Tecnológica en el Banco Nacional de Bolivia. Anteriormente en la empresa DATACOM S.A. como técnica de proyectos especiales (2017).
Email: helen.vallejos.q@gmail.com.