

**ITESO**

Universidad Jesuita de Guadalajara

HoneyPot

**Equipo número:** 2

**Presentado por**:

Gustavo Rivas Lucano | Jorge Darío García Jaime

**Correo Electrónico:**

[gustavo.rivas@iteso.mx](mailto:gustavo.rivas@iteso.mx) | [is722395@iteso.mx](mailto:is722395@iteso.mx)

**Para el curso de**: Cloud Computing (Development)

**Impartida por**: Mtro. Ojeda Orozco Miguel Angel

**Fecha**: 11/06/2024

**Nombre del proyecto**

AWS HoneyPot

**Marco Teórico**

La seguridad en la informática es una preocupación creciente a medida que más sistemas y datos críticos se migran a la nube. Los honeypots son herramientas de seguridad utilizadas para detectar, desviar y estudiar intentos de ataque cibernético, y su implementación en la nube presenta nuevas oportunidades y desafíos.

Definición y Objetivo de los Honeypots

Un honeypot es un sistema diseñado para atraer a los atacantes y permitir el monitoreo y análisis de sus acciones. Su principal objetivo es recopilar información sobre técnicas y tácticas de los atacantes, así como detectar y mitigar amenazas antes de que afecten a los sistemas reales .

3. Servicios de AWS Utilizados

3.1 Amazon EC2

Amazon Elastic Compute Cloud (EC2) es un servicio web que proporciona capacidad de computación escalable en la nube. En este proyecto, se utiliza una instancia EC2 para desplegar el honeypot, configurando un entorno controlado que atraiga a los atacantes.

3.2 AWS Lambda

AWS Lambda es un servicio de cómputo que ejecuta código en respuesta a eventos y gestiona automáticamente los recursos de cómputo subyacentes. En este proyecto, Lambda se utiliza para procesar y analizar los registros de los intentos de ataque almacenados en Amazon S3.

3.3 Amazon S3

Amazon Simple Storage Service (S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos y seguridad. Los registros generados por el honeypot en EC2 se almacenan en S3 para su análisis posterior.

3.4 AWS Glue

AWS Glue es un servicio de integración de datos que facilita la preparación y carga de datos para su análisis. En este proyecto, Glue se utiliza para transformar y catalogar los registros almacenados en S3, preparándolos para consultas y análisis.

3.5 Amazon Athena

Amazon Athena es un servicio de consulta interactiva que permite analizar datos directamente en Amazon S3 utilizando SQL estándar. Athena se utiliza para ejecutar consultas sobre los datos transformados, permitiendo identificar patrones y tendencias en los intentos de ataque.

4. Implementación del Honeypot

4.1 Configuración de la Instancia EC2

Se despliega una instancia EC2 con una configuración mínima de seguridad para simular un servidor vulnerable. El software honeypot, como Cowrie, se instala y configura en esta instancia para registrar actividades maliciosas.

4.2 Almacenamiento y Procesamiento de Registros

Los registros generados por el honeypot se transfieren periódicamente a un bucket de Amazon S3. Una función AWS Lambda se encarga de procesar estos registros, extrayendo datos relevantes y almacenándolos en un formato estructurado.

4.3 Transformación y Análisis de Datos

AWS Glue se utiliza para catalogar y transformar los registros en S3, convirtiéndolos en un formato adecuado para el análisis con Amazon Athena. Athena permite ejecutar consultas SQL sobre los datos transformados, facilitando la identificación de patrones de ataque.

**Requerimientos**

<Requerimientos técnicos del proyecto>

**Diagrama**

<Creado con los íconos de la documentación oficial de AWS)

**Desarrollo del proyecto**

<Descripción de todos los pasos realizados durante el desarrollo del proyecto; incluyendo capturas de pantalla>

**Costo**

<Costo estimado mensual para la propuesta del proyecto>.

**Conclusiones**

La implementación de honeypots en la nube ofrece una poderosa herramienta para la detección y análisis de ciberataques. A pesar de los desafíos que presenta, su capacidad para escalar y adaptarse rápidamente a nuevas amenazas los convierte en una parte integral de las estrategias de seguridad moderna.

**Bibliografía**

<Correctamente referenciada en todos los apartados (marco teórico, requerimientos, desarrollo etc.) donde haya sido utilizada>