UIDE
Powered by
Arizona State University

*Maestría en*

# CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

**AUTORES:** Ing. Mario David Sigcha Morochz

Ing. Darling Camila Arroyo Pérez

Ing. Juan Paulo Escobar Calderón

**TUTOR:** Ing. Ronie Stalin Martínez Gordon, Mtr.

## Investigación de nuevas tendencias de ataques y defensa con SIEM y Hacking Ético.

QUITO – ECUADOR | 2024

## RESUMEN

En el proyecto de investigación, previo a la obtención del título de Magister en Ciberseguridad, se realizó un análisis de las tendencias de ataques informáticos en la nube con la implementación de un honeypot T-Pot en una máquina virtual dentro de la plataforma Google Cloud. El estudio permitió determinar el tipo de ataque más recurrente en la nube, proponer posibles soluciones adaptadas a dicho tipo de ataque, y evaluar las ventajas y desventajas de diferentes tipos de honeypots. De esta manera, se puede determinar el tipo de honeypot más adecuado para una infraestructura especifica según el escenario. El honeypot T-pot implementado en la nube, específicamente sobre la plataforma Google Cloud, consta de una máquina virtual con 4 vCPU, 2 core, 16 GB RAM, Sistema Operativo "Debian GNU/Linux 11 (bullseye), x86/64, amd64 built on 20240312" y un disco de almacenamiento de 499 GB, el firewall que protege al T-Pot está configurado con todos los puertos TCP y UDP abiertos, con el objetivo de recolectar una amplia gama de datos. Finalmente, la evaluación del honeypot T-Pot se llevó a cabo con el análisis de la cantidad de ataques, con el histograma de dichos ataques, con los países de origen donde se generaron los ataques y con los puertos más utilizados por los atacantes, dependiendo del honeypot del T-Pot durante un periodo de quince días, comprendido del 16 al 30 de marzo del 2024 y, en otro periodo, del 16 de marzo del 2024 al 16 de abril del 2024 se obtuvo únicamente la cantidad de ataques recibidos. Se investigó acerca de las herramientas de seguridad para la prevención de los ataques cibernéticos más recurrentes detectados.

**PALABRAS CLAVE**

- **HONEYPOT**
- **T-POT**
- **ATAQUE INFORMÁTICO**
- **DDOS**
- **SIEM**

## ABSTRACT

In the research project, prior to obtaining the master's degree in Cybersecurity, an analysis of the trends of computer attacks in the cloud was carried out with the implementation of a T-Pot honeypot in a virtual machine within the Google Cloud platform. The study made possible to determine the most recurrent type of attack in the cloud, propose possible solutions adapted to said type of attack, and evaluate the advantages and disadvantages of different types of honeypots. Therefore, the most appropriate type of honeypot for a specific infrastructure can be determined depending on the scenario. The T-pot honeypot implemented in the cloud, specifically on the Google Cloud platform, consists of a virtual machine with 4 vCPU, 2 core, 16 GB RAM, Operating System "Debian GNU/Linux 11 (bullseye), x86/64, amd64 built on 20240312" and a 499 GB storage disk, the firewall that protects the T-Pot is configured with all TCP and UDP ports open, with the aim of collecting a wide range of data. Finally, the evaluation of the T-Pot honeypot was carried out with the analysis of the number of attacks, with the histogram of those attacks, with the countries of origin and with the ports most used by the attackers, depending of the T-Pot honeypot during a period of fifteen days, from March 16 to March 30 2024 and, in another period, from March 16 2024 to April 16 2024, only the number of attacks received was obtained. The security tools for preventing the most recurrent cyber-attacks detected were investigated.



**KEYWORDS**

- **HONEYPOT**
- **T-POT**
- **COMPUTER ATTACK**
- **DDOS**
- **SIEM**