



Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES:

- Ing. Francisco Javier Hermosa Machado
- Ing. David Alejandro Vilatuña Chisaguano
- Ing. Sebastián Darío Llerena Granda
- Ing. Gerardo Patricio Jiménez Coral

DIRECTOR: Ing. Alejandro Cortés

**IMPLEMENTACIÓN DE UN HONEYPOT PARA LA DETECCIÓN, ANÁLISIS
Y FORTALECIMIENTO DE LA SEGURIDAD CIBERNETICA
DE LA EMPRESA SATURNO COMPUTING SERVICES “SATURNOCS S.A.”**

Resumen

Los autores tienen como finalidad utilizar una de las herramientas más representativas de la ingeniería del engaño, que permite mezclarse dentro de los recursos de la empresa, con ello podremos detectar personas que hayan vulnerado las seguridades tradicionales, esta técnica proporciona información a los equipos de TI para conocer a los atacantes, identificando patrones de acción y combatirlos, con estos resultados encontrados hemos elaborado recomendaciones de ciberseguridad a medida para la empresa Saturno Computing Services.

Para el desarrollo, los autores abordan conceptos básicos de ciberseguridad, como los tipos de ataques que se encuentran expuestas las empresas en estos momentos, al igual que la descripción de las seguridades tradicionales que son implementadas.

Los autores se enfocan en una solución que fue creada tiempo atrás, pese a ello, no ha sido explotada en toda su amplitud siendo este el Honeypot.

Adicionalmente los autores con la información obtenida han elaborado implementos adicionales que dan valor agregado a la empresa, para no solo tener recomendaciones en los servicios ya implementados, sino conocer potenciales riesgos de ciberseguridad a servicios que tienen en la planificación a mediano y largo plazo.

Finalmente, con esta información también se podrán implementar por parte de la empresa buenas prácticas que brinden la seguridad en dichos servicios.

Palabras Clave:

Honeypot, ciberseguridad, ciber ataques, herramientas de ciberseguridad.

Abstract

The authors intend to use one of the most representative tools of deception engineering, which allows mixing within the company's resources, with this we will be able to detect people who have violated traditional security, this technique provides information to IT teams to know the attackers, identifying patterns of action and combating them, with these results, we have developed tailor-made cybersecurity recommendations for the company Saturno Computing Services.

For the development, the authors address basic cybersecurity concepts, such as the types of attacks that companies are exposed to now, as well as the description of the traditional securities that are implemented.

The authors focus on a solution that was created some time ago, despite this, it has not been exploited to its full extent, this being the Honeypot.

Additionally, the authors, with the information obtained, have developed additional implements that give added value to the company, to not only have recommendations on the services already implemented, but also to know potential cybersecurity risks to services that they have in the medium- and long-term planning.

Finally, with this information, the company will also be able to implement good practices that provide security in these services.

Keywords:

Honeypot, cybersecurity, cyber-attacks, cybersecurity tools.