Resumen

El objetivo de la presente investigación es desarrollar un prototipo de detección y priorización de vulnerabilidades basado en Shodan, a través de una arquitectura Cliente-Servidor para los servicios reactivos y proactivos del ESPE-CERT. En primer lugar, se revisó de forma sistemática los enfoques, técnicas y herramientas en la implementación de sistemas de detección y escaneo de vulnerabilidades, por medio de la guía metodológica de Barbara Kitchenham. Los resultados demostraron que no existe una metodología estándar o predominante para el proceso de desarrollo, por lo cual se propuso una metodología con cinco fases y un proceso de desarrollo con seis fases para los sistemas de detección de vulnerabilidades. En segundo lugar, a través de la metodología OSINT se aplicaron las fases de colección, análisis y extracción de conocimiento. Los datos de entrada se obtuvieron a través de las REST API de Shodan, luego se aplicó un proceso matemático con la información relevante sobre vulnerabilidades y su entorno para poder cuantificar y calcular el factor de riesgo de cada vulnerabildad, logrando un orden de priorización. En tercer lugar, se construyó un servicio web mediante el modelo de prototipos, que permita extraer, correlacionar y analizar la información. Los resultados muestran que Shodan tiene variables relevantes la cuales permiten evaluar y cuantificar la sobreexposición información de una organización. Además, se identificó que CVSS no es suficiente para priorizar vulnerabilidades, ya que los entornos donde se identifican tienen características diferentes. Finalmente este estudio aporta con metodologías, un modelo de priorización y un prototipo para los servicios del ESPE-CERT.

Palabras clave:

- **DETECCIÓN DE VULNERABILIDADES**
- **CIBERSEGURIDAD**
- **SHODAN**

Abstract

The objective of the present research is to develop a prototype of vulnerability detection and prioritization based on Shodan information, through a Client-Server architecture for ESPE-CERT's reactive and proactive services. First, approaches, techniques and tools in the implementation of vulnerability detection and scanning systems were systematically reviewed through Barbara Kitchenham's methodological guide. The results showed that there is no standard or predominant methodology for the development process, so a five-phase methodology and a six-phase development process for vulnerability detection systems were proposed. Secondly, through the OSINT methodology, the phases of knowledge collection, analysis and extraction were applied. The input data were obtained through Shodan's REST APIs, then a mathematical process was applied with the relevant information on vulnerabilities and their environment in order to quantify and calculate the risk factor of each vulnerability, achieving an order of prioritization. Thirdly, a web service was built using the prototype model to extract, correlate and analyze the information. The results show that Shodan has relevant variables which allow to evaluate and quantify the information overexposure of an organization. In addition, it was identified that CVSS is not sufficient to prioritize vulnerabilities, since the environments where they are identified have different characteristics. Finally, this study provides methodologies, a prioritization model and a prototype for ESPE-CERT's proactive and reactive services.

Keywords:

- **VULNERABILITY DETECTION**
- **CYBERSECURITY**
- **SHODAN**