FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Implementación de un sistema de monitoreo de modificaciones de los registros DNS empleando software libre para detectar alteraciones ilícitas de los servidores de nombre de dominio, en la empresa Taapaq EIRL

Autor:
Bach. Neira Basso, Francisco Javier

Asesor:
Ing. Luis Angel Camacho Colán

Pimentel, 01 de agosto del 2014

RESUMEN

La presente investigación, titulada “Implementación de un sistema de monitoreo de modificaciones de los registros DNS empleando software libre para detectar alteraciones ilícitas de los servidores de nombre de dominio” surge a raíz de una debilidad observada por el tesista cuando tuvo oportunidad de observar de cerca e interactuar con otros oficiales de seguridad de la información.

El objetivo de este trabajo es implementar un sistema sencillo de instalar y operar, que requiera del mínimo de “housekeeping” pero que a la vez sea sumamente confiable y que reporte eficazmente todo cambio sobre los servidores de nombres de dominio, sean autorizados o no, registre el evento y luego pasar a condición “verde” si se le reporta que el cambio fue lícito.

Con la finalidad de que este sistema sea difundido entre los distintos equipos de respuesta a incidentes sin incurrir en pagos por licenciamiento, este sistema está elaborado con software libre.

ABSTRACT

This project, “An Implementation of a Modification Monitoring System for DNS Records Using Free software to Detect Unauthorized Modifications to the Domain Name Servers” is intended to be a possible countermeasure to a vulnerability observed by the author during an incident where he had the opportunity to closely observe and interact with other information security officers.

The objective of this work is to implement a monitoring system that is simple to install and to operate, that requires the minimum of housekeeping, but at the same time is highly reliable and dependably reports every change, authorized or not, to the domain name servers, logs the event, and reports a “green" condition if the modification was legitimate.

In order for this system to be distributed among the various computer incident response teams without incurring licensing payments, this system is built using free software.