RESUMEN DE LA TESIS

IMPLEMENTAR UNA RED HONEYPOTS PARA DETECCIÓN Y CLASIFICACIÓN DE INTRUSOS MEDIANTE MÁQUINAS VIRTUALES EN EL MINISTERIO DE DEFENSA NACIONAL

En la actualidad las redes informáticas se encuentran expuestas a ataques y robos de información generando grandes daños económicos y problemas en el funcionamiento de la red. La presente investigación analiza la implementación de una herramienta de seguridad informática denominada Honeypost, utilizando plataformas de virtualización. Esta herramienta permite realizar el control, captura y análisis de los datos recolectados, lo cual permite establecer las formas de ataque, de dónde se realiza la intrusión y los mecanismos para poder disminuir dichos ataques. Para la ejecución de esta investigación se instaló el honeynet virtual autocontenida de tercera generación, se implementó tres honeypost con diferentes sistemas operativos y servicios, los mismos que presentaban vulnerabilidades para atraer a los intrusos. La máquina fuente se conectó directamente al router de la empresa, con el fin de evitar daños en la red de producción. Además se realizaron pruebas de escaneo, fuerza bruta y denegación de servicio. El Honeynet registró las intrucciones a la red y el comportamiento de los atacantes, lo que ayudó a establecer mecanismos de mejora en la seguridad requerida.

Palabras claves: ataques, vulnerabilidad, redes de información, virtualización, honeypots.

Abstract

Nowadays the computer networks are not only exposed to attacks, but also to information theft which have been generating huge economics damages, and troubles in the network working. This research analyzes the implementation of a security computer tool called "Honeypost", using virtualization platforms. What this tool allows is to monitor, capture and analyze a group of collected data through which permit to establish the different forms of attack, from which is the intrusión performed and the mechanics to reduce such attacks. In order to run this computer research, the third generation of self- contained virtual was installed. Besides, it was implemented three honeypost with different operanting systems and services. these have showed vulnerabilities to attrack intruders. The source machine was directly connected to the router of the company in order to avoid damages in the production network. It was therefore done scanning tests, brute force and rejection of the service. Finally, the Honeynet registered the intrusions to the network and behavior of the attackers what helped to establish the mechanics for improving the required security.

Keywords : attack, vulnerability , information networks , virtualization, honeypots.