Resumen

Hoy en día los constantes avances tecnológicos y la interconexión global de dispositivos a través de Internet han abierto un mundo de oportunidades para que las personas realicen tareas que hace algunos años eran impensables. A medida que el tiempo transcurre los dispositivos inteligentes van tomando mayor aceptación y generan mayor utilidad al ser humano, abarcando tanto sectores industriales como domésticos. En consecuencia, nuevas técnicas de intrusión van apareciendo, generando nuevas vulnerabilidades de seguridad informática.

Los dispositivos IoT en la actualidad pueden utilizarse como agentes para difundir ataques informáticos a pequeña y gran escala. Evidentemente, es necesario afrontar estos nuevos retos de seguridad cibernética en los productos y servicios del Internet de las Cosas creando medidas para prevenir y detectar ciberataques en estos entornos. El propósito del presente trabajo es realizar el análisis de vulnerabilidades de seguridad informática en entornos IoT a través de honeypots. Para lo cual, se implementó un MHN (Modern Honey Network) el cual es un servidor centralizado para la administración y recopilación de datos de honeypots. Mediante una honeynet virtual autocontenida y una Raspberry pi se instalaron tres señuelos diferentes. Los honeypots instalados simulan servicios atractivos e intencionalmente expuestos para ser atacados por un ciberdelincuente. Estos señuelos están implementados dentro de un escenario real de un invernadero inteligente y se harán pasar como servidores de producción dentro de la red IoT. Con este escenario de prueba se comprobará la capacidad de detección de los honeypots. La finalidad es obtener un sistema que pueda identificar las técnicas utilizadas por los cibercriminales en ataques internos o externos a las redes del Internet de las Cosas.

Palabras clave: honeypot, ciberseguridad, IoT, vulnerabilidad, auditoría de seguridad informática.

Abstract

Nowadays, constant technological advances and the global interconnection of devices through the Internet have opened up a world of opportunities for people to perform tasks that were unthinkable a few years ago. As time goes by, smart devices are becoming more accepted and more useful to humans, covering both industrial and domestic sectors. As a result, new intrusion techniques are emerging, creating new computer security vulnerabilities.

IoT devices can nowadays be used as agents to spread small- and large-scale cyber-attacks. Clearly, it is necessary to address these new cyber security challenges in Internet of Things products and services by creating measures to prevent and detect cyber-attacks in these environments. The purpose of this work is to perform the analysis of cyber security vulnerabilities in IoT environments through honeypots. For this purpose, a MHN (Modern Honey Network) was implemented, which is a centralized server for the administration and collection of honeypot data, and by means of a self-contained virtual honeynet and a Raspberry Pi, three different decoys were installed. The installed honeypots simulate attractive and intentionally exposed services to be attacked by a cybercriminal. These decoys are implemented within a real scenario of a smart greenhouse and will masquerade as production servers within the IoT network. This test scenario will be used to test the detection capability of the honeypots. The aim is to obtain a system that can identify the techniques used by cybercriminals in internal or external attacks on Internet of Things networks.

Keywords: honeypot, cybersecurity, IoT, vulnerability, IT security audit.