

Resumen

El presente estudio se llevó a cabo para cubrir la necesidad que tienen los hogares y pequeñas microempresas para la protección de datos. Para lograrlo, se diseñó y configuró en una placa electrónica de circuitos compacta o SBC (SINGLE BOARD COMPUTER) con una Gestión Unificada de Amenazas (Unified Threat Management, UTM) que ofrece algunas funcionalidades de protección de la información de bajo costo. Específicamente, tanto las funciones de detección y prevención de intrusos, como la de filtrado de contenido (firewalling). Para su ejecución se aplicó la Metodología de Investigación acción, y el uso de varias herramientas de hardware y software de código abierto (open-source) tanto para la recolección, inyección, filtrado y análisis de tráfico. Para las pruebas de concepto se utilizaron entornos virtuales de red controlados, sobre el cual se inyectaron diferentes tipos de ataques a la red. Los resultados demostraron la efectiva funcionalidad del UTM implementado sobre el hardware libre Atomic Pi.

- Palabras claves:

- **UTM**
- **ATOMIC PI**
- **CLEAROS**
- **METASPLOIT**

Abstract

This study was conducted to cover the need of households and small micro-enterprises for data protection. To carry out this, a Unified Threat Management (UTM) was designed and configured on a compact electronic circuit board (SBC), which offers some low-cost information protection functionalities. Specifically, both intrusion detection and prevention functions, as well as content filtering (firewalling). For its execution, the Action Research Methodology was applied, and the use of various hardware and open-source tools for the collection, injection, filtering, and analysis of traffic. A controlled virtual network environment was then used for the proofs of concept, on which different types of network attacks were injected. The results demonstrated the practical functionality of the UTM implemented on the free Atomic Pi hardware.

- Key words:

- **UTM**
- **ATOMIC PI**
- **CLEAROS**
- **METASPLOIT**