RESUMEN

El propósito del presente trabajo es hacer un análisis de la red de datos de la organización Youphone Cia. Ltda. Esto es realizando un levantamiento de la información del equipamiento informático y de los equipos usados en la red de datos, al tener todos estos datos se hacen varias pruebas de hacking ético en sus diferentes fases como son reconocimiento, exploración, acceso en sus dos pasos, y cubrir huellas. Se ocupa una metodología de checklist con diferentes puntos que se mostrarán en el transcurso del presente documento, con los resultados encontrados se trata de minimizar o eliminar las brechas de seguridad, dictando las políticas de seguridad y la manera de socializarlas a todos los empleados de la empresa. Para lo mencionado se utilizan programas libres y bajo licencia que permiten visualizar resultados para las diferentes fases del hacking ético.

Estas pruebas se realizan sobre todos los servidores de la organización, esto es 2 servidores en el Cavs Condado, 1 servidor en el Cavs CCI y aleatoriamente a 10 computadores de usuarios en los 3 distintos lugares, de ventas de la empresa los resultados obtenidos se tabulan, se analizan y se entrega un informe o Resumen ejecutivo a gerencia con recomendaciones que se deben implementar en la empresa.

Palabras Clave:

- **CHECKLIST**
- **BRECHAS DE SEGURIDAD**
- **POLÍTICAS DE SEGURIDAD**
- **HACKING ÉTICO**

ABSTRACT

The present research has the main objective of the Analysis and Diagnostic of networking vulnerabilities of Youphone CIA. Among techniques, tools and procedures of ethical hacking in order to issue recommendations that will minimize the associated risk. Youphone is a retailer of Telefónica which is dedicated to sells cell phones and mobile plans. This enterprise is affected by the long waiting for transactions, suspension of service during peak hours and stolen information. Due to these facts this project was based on the Ethical Hacking Model under OSSTMM methodology (open source security Testing Methodology Manual) using CheckLists.The tools used during this project were free software and under license. Among the free tools can be mentioned Wireshark, Advanced Port Scanner, AngryIPScanner, etc On the other hand; the licensed tools used were those that allow in a limited time such as Nessus and VisualRoute. The final results allowed us to find security fails basically centered on open ports. Based on this, an optimization and prioritization of network traffic plan and Executive inform were issued in which procedures and recommendations were detailed in order to protect the company from future informatics attacks.

KeyWords:

- **ETHICAL HACKING**
- **OSSTMM**
- **CHECKLIST**
- **SECURITY'S HOLES**
- **OPTIMIZATION AND PRIORITIZATION PLAN**