Universidad Tecnológica de México

MAESTRÍA EN SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN

HACKING ÉTICO Y ANÁLISIS FORENSE

2023-03

CAMPUS SUR

PROFESOR MAESTRO RODRÍGUEZ AGUILAR BENITO ALAN

ENTREGABLE FINAL: “PROPUESTA DE REPORTE DE HACKEO ÉTICO Y DE CÓMPUTO FORENSE”

ALUMNA KUHLIGER MARTÍNEZ MARTHA GUADALUPE

NÚMERO DE CUENTA: 334011227

30 DE JULIO DEL 2023

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente documento permitió reforzar y poner en práctica los conceptos que se aprendieron en el curso de Hacking Ético y Análisis Forense mediane el desarrollo de una propuesta que dará solución a una problemática y mejorará la seguridad de una organización, la cual se llamará R&K Audit para este caso de estudio.

Este caso de estudio consistió en detectar vulnerabilidades a través de pruebas de penetración aplicando conocimientos y principios de Hacking Ético, con el propósito de proteger a la organización y guiarla para detectar sus vulnerabilidades y prevenir ataques dañinos causados por los ciberdelincuentes.

Se realizó una investigación sobre herramientas que se implementaron, así como las plataformas de búsqueda de vulnerabilidades, se instaló el sistema operativo Kali Linux y la máquina virtual Metasploitable 2, se ejecutaron pruebas de penetración para detectar vulnerabilidades, se desarrolló un análisis de vulnerabilidades para calcular el impacto y la probabilidad con la ayuda de aplicación OWASP Risk Rating Calculator y se desarrolló una matriz de riesgos. Además, se analizó una imagen forense, donde se obtuvo la dirección IP del equipo, el nombre de los usuarios y la última vez que iniciaron sesión, el número de serie del disco duro, el historial de Internet Explorer, el nombre y la ubicación de los archivos enviados a la papelería de reciclaje y los corros electrónicos de una cuenta de Outlook.

Con base a lo mencionado anterior se desarrolló una propuesta que garantizará una mayor seguridad en los sistemas y equipos informáticos de la organización R&K Audit. También se describen soluciones y recomendaciones para corregir las vulnerabilidades que se detectaron en los sistemas del Departamento de Asesoría en Riesgo.

Por confidencialidad se ha modificado el nombre de la organización R&K Audit.

ABSTRACT

This document allowed to reinforce and put into practice the concepts learned in the course of *Ethical Hacking and Forensic Analysis* through the development of a proposal that will provide a solution to a problem and improve the security of an organization, which will be called *R&K Audit* for this case study.

This case study consisted of detecting vulnerabilities through penetration testing by applying knowledge and principles of Ethical Hacking, in order to protect the organization and guide it to detect its vulnerabilities and prevent harmful attacks caused by cybercriminals.

An investigation was conducted on tools that were implemented, as well as vulnerability search platforms, the Kali Linux operating system and the Metasploitable 2 virtual machine were installed, penetration tests were executed to detect vulnerabilities, a vulnerability analysis was developed to calculate the impact and probability with the help of OWASP Risk Rating Calculator application and a risk matrix was developed. In addition, a forensic image was analyzed, where the IP address of the computer, the name of the users and the last time they logged in, the serial number of the hard disk, the history of Internet Explorer, the name and location of the files sent to the recycle bin and the e-mails from an Outlook account were obtained.

Based on, a proposal was developed to ensure greater security in the computer systems and equipment of the R&K Audit organization. It also describes solutions and recommendations to correct the vulnerabilities detected in the systems of the Risk Advisory Department.

For confidentiality reasons, the name of the R&K Audit organization has been changed.