UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Trabajo Final de Maestría previa a la obtención del título de Magíster en Ciberseguridad

AUTOR: Ing. William Daniel Carrera Arias
Lic. René Alexander López Peralta
Ing. Diego Andrés Noboa Yánez
Ing. Christian Néstor Vega Muñoz

TUTOR: Ing. Alejandro Cortés.Msc

Ejecución y Análisis de un ejercicio de RED TEAM para el GAD de Tulcán, para la identificación de vulnerabilidades, debilidades y vectores de ataque, que puedan afectar a la disponibilidad, confidencialidad e integridad de la información de la institución.

QUITO – ECUADOR | 2023

Resumen

El presente ejercicio de "RED TEAM", tiene como principal objetivo, detallar a manera de análisis el estado actual de un GAD Municipal, frente a lo que conlleva la seguridad informática. Las fases planeadas y ejecutadas en el presente ejercicio son:

Ingeniería social, con suplantación de identidad bajo phishing en correo electrónico utilizando Gophish, tomando una muestra de 149 usuarios internos de la organización, realizada desde el 23 de marzo al 25 de mayo del 2023.

Reconocimiento y análisis externo e interno del GAD Municipal mediante el uso de técnicas de Ethical Hacking y Pentesting utilizando un conjunto de herramientas entre las que destacan Nessus y Herramientas internas del sistema como Responder, CrackMapExec, MetaExploit, etc. bajo estándares PTEST y OWASP, análisis de vulnerabilidades, explotación controlada, toma de control de activos internos, captura de información sensible como usuarios y contraseñas, accesos validos con información obtenida, esto de la mano de la identificación actual del vector de ataque aplicable en la organización.

Obteniendo como resultado, entre los entregables un Plan de Remediación que permita a la toma de decisiones a corto y largo plazo, permitiendo la mejora de la Ciber-Postura dentro de la organización.

Palabras Clave

Red Team, Ingeniería social, análisis, vulnerabilidades, explotación.

Abstract

The main objective of this "RED TEAM" exercise is to analyze the current state of a Municipal Government in terms of information security. The phases planned and executed in this exercise are:

Social engineering with impersonation under phishing in email using Gophish, taking a sample of 149 internal users of the organization, was carried out from March 23 to May 25, 2023. Recognition and external and internal analysis of the Municipal GAD through the use of Ethical Hacking and Pentesting techniques using a set of tools including Nessus and internal system tools such as Responder, CrackMapExec, MetaExploit, etc. under PTEST and OWASP standards, vulnerability analysis, controlled exploitation, taking control of internal assets, capture of sensitive information such as users and passwords, and valid access with the information obtained, all hand in hand with the current identification of the attack vector applicable in the organization.

As a result, among the deliverables, a Remediation Plan that permits short and long term decision-making, allowing the improvement of the cyber posture within the organization was presented.

Keywords

Red Team, Social engineering, analysis, vulnerabilities, exploitation.