Resumen

A partir de la Convocatoria 2020 para proyectos de investigación aplicada la Universidad de las Fuerzas Armadas ESPE comenzó un proceso de implementación de un CERT así como del EGSI que viene desarrollando la Unidad de Seguridad Integrada de la ESPE, junto con estas implementaciones surgió la problemática de crear un equipo dedicado a la realización de pruebas de penetración es decir Hacking Ético que funcione bajo el CERT utilizando ITIL V4, en donde se utilizó como casos de empleo las aplicaciones críticas de la Universidad de las Fuerzas Armadas ESPE brindados por el EGSI de la universidad, todo esto con el fin de implantar esta capacidad como servicio a otras universidades o instituciones. El proyecto de tesis se basó en el hacking de sombrero blanco que viene a ser el hacking ético, es decir, aquel hacking que se rige por leyes judiciales y morales dentro de un contrato establecido entre la organización y el hacker, cuya diferencia respecto al cracking se basa en la finalidad, ya que si bien es cierto que en procedimiento son iguales, su finalidad es muy distinta, la finalidad de un hacker ético es encontrar brechas en la seguridad de dentro del sistema o aplicativo para su posterior corrección y mejora de la organización, el cracker por su parte, puede tener varios objetivos, desde el daño a la organización, fines de lucro, o incluso el de la mera prueba de sus habilidades con cracker. El desarrollo práctico de la tesis constó de seis fases para realizar un correcto servicio de hacking ético, los cuales son: Establecimiento del anonimato, Recopilación de Información, Escaneo, Explotación, Mantenimiento del Acceso y evaluación del servicio en donde se realiza un informe de no conformidades explicando los resultados de la praxis.

Palabras clave: CERT, servicio de TI, Hacking ético, gestión de servicio ITIL

Abstract:

Starting from the 2020 Call for Applied Research Projects, the Universidad de las Fuerzas Armadas ESPE began the implementation process of a CERT as well as the EGSI being developed by the ESPE's Integrated Security Unit. Along with these implementations, the problem arose of creating a team dedicated to carrying out penetration testing, that is, ethical hacking that operates under the CERT using ITIL V4. Critical applications of the University of the Armed Forces ESPE provided by the university's EGSI were used as use cases to implant this capability as a service to other universities or institutions. The thesis project was based on white hat hacking, which is ethical hacking that follows legal and moral rules within a contract initially established between the organization and the ethical hacker. The difference between ethical hacking and cracking is based on their purpose, as although their procedures are similar, their purposes are very different. The purpose of an ethical hacker is to find security breaches within the system or application for subsequent correction and improvement of the organization. The cracker, on the other hand, can have various objectives in mind, from harming the organization, for-profit purposes, or even just for testing their skills as a cracker. The practical development of the thesis consisted of six phases to provide a correct ethical hacking service, which are: Establishment of Anonymity, Information Gathering, Scanning, Exploitation (i.e., establishing access), Access Maintenance (a phase that was not reached due to the platform's security), and Service Evaluation where a report of non-conformities is produced explaining the results of the practice.

Key words: CERT, IT service, Ethical Hacking, ITIL service management