**Maestría en**

## Ciberseguridad

**Trabajo previo a la obtención de título de**

**Magister en Ciberseguridad**


**AUTOR/ES:**

Santiago Efraín Arteaga Egas

Alex Giovanny Chugchilán Cachago

Jorge Iván Guijarro Altamirano

Josue Vladimir Morales Rivera

Marco Andrés Rodríguez Solís

**TUTOR/ES:**

Alejandro Cortés López

Iván Reyes Chacón


**TEMA:**

Pentesting en el Hipervisor VMware ESXi y contenedor Kubernetes utilizando herramientas de escaneo y penetración

REINVENTEMOS EL FUTURO

## RESUMEN

El presente proyecto tiene como objetivo realizar pruebas de penetración (pentesting) en infraestructuras virtualizadas que utilizan el hipervisor VMware ESXi y contenedores Kubernetes, con el fin de identificar vulnerabilidades que puedan comprometer la seguridad de estos entornos. La investigación se enfoca en el uso de herramientas especializadas de escaneo y penetración, tales como Metasploit, Nmap y escaners específicos de Kubernetes, dentro de un entorno de laboratorio controlado. La justificación del estudio radica en el crecimiento exponencial del uso de tecnologías de virtualización y contenedores en entornos empresariales y de nube, lo que exige una evaluación continua de su postura de seguridad. A través de una metodología práctica y sistemática, se espera identificar vectores de ataque críticos y proponer recomendaciones de mitigación. Los resultados buscan contribuir al fortalecimiento de la ciberseguridad en arquitecturas modernas de infraestructura TI.

Palabras Claves: Hipervisores, Contenedores, VMware ESXi, Kubernetes, Pentesting

## ABSTRACT

This project aims to perform penetration testing (pentesting) on virtualized infrastructures using the VMware ESXi hypervisor and Kubernetes containers, in order to identify vulnerabilities that may compromise the security of these environments. The research focuses on the use of specialized scanning and penetration tools, such as Metasploit, Nmap and Kubernetes-specific scanners, within a controlled laboratory environment. The rationale for the study lies in the exponential growth of the use of virtualization and container technologies in enterprise and cloud environments, which demands a continuous assessment of their security posture. Through a practical and systematic methodology, it is expected to identify critical attack vectors and propose mitigation recommendations. The results seek to contribute to the strengthening of cybersecurity in modern IT infrastructure architectures.

Keywords: Hypervisors, Containers, VMware ESXi, Kubernetes, Pentesting