Resumen

El presente proyecto, describe la implementación, experimentación y mitigación de técnicas de escaneo de puertos sobre una infraestructura virtualizada. Para el diseño de esta infraestructura se utilizó la normativa ISO 27004 y para la fase de experimentación, se tomó la metodología OSSTMM v3.0 para toma de muestras y cuantificación de los resultados. Los resultados obtenidos han sido el producto de la experimentación con soluciones propuestas en este trabajo, que tienen por objetivo mitigar el escaneo de puertos, para lo cual, se realizó dichos experimentos con herramientas que permitan el ataque y la cuantificación de los resultados, como lo son NMAP y Wireshark respectivamente. Por esto, se ha logrado medir el envío de paquetes, medición de banda ancha, tiempos de retardo y adquirir topologías de la infraestructura.

Finalmente, se ha logrado mitigar los ataques con un porcentaje del 96% de éxito, tomando en cuenta que la detección de patrones y el bloqueo del tráfico generado pueden afectar las comunicaciones del laboratorio de pruebas. Es por esto, que los tiempos de retardo son una métrica sensible a este tipo de solución, por lo tanto, filtrar e identificar un ataque implica un aumento en el tiempo que se necesita para realizar una comunicación exitosa entre un emisor y receptor. Todos estos aspectos han sido debidamente analizados en este trabajo y han sido probados en su totalidad en un laboratorio de máquinas virtuales.