RESUMEN

El continuo aparecimiento de diversas amenazas, vulnerabilidades y tipos de ataques que implican hurto, modificación, espionaje, interrupción, falsificación, denegación de servicios etc., en las redes TCP/IP, perjudica directamente a los negocios que son altamente dependientes de sus sistemas y redes de información.

Para prevenir y contrarrestar una amplia gama de amenazas a las seguridades de las redes TCP/IP, es necesario conocer sus vulnerabilidades e identificar diversos tipos de ataques. Para manejar esta situación se propone crear un ambiente de red controlado con los componentes necesarios que detecten ataques maliciosos, para analizarlos y contrarrestarlos, a través de la utilización de máquinas virtuales, con las cuales es posible reducir costos de inversión de hardware, costos de mantenimiento, costo y tiempo de experimentación y sobre todo reduciría el riesgo del colapso de la red en producción.

El presente trabajo tiene como objetivo diseñar e implementar una plataforma de experimentación para evaluar ataques reales de redes IP utilizando plataformas de virtualización de libre distribución e implementar mecanismos de control y mitigación para contrarrestarlos. Para llevarlo a cabo, se diseñó e implementó dos escenarios de experimentación utilizado VMware Player y VirtualBox. Luego se aplicó diversos tipos de ataques a cada escenario creado. Posteriormente se evaluó el impacto que provocan los diversos ataques analizando la información de las trazas. Finalmente se proponen mecanismos de mitigación de cada uno de estos ataques. Todo esto utilizando diversas herramientas de código abierto y de libre distribución.