RESUMEN

Las redes inalámbricas tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red cableada. Sin embargo, su punto débil reside en la característica que la hace tan popular: la transmisión por un medio público como es el aire.

En el presente trabajo se realiza una investigación del estado del arte en la detección de intrusiones en redes inalámbricas. En primer lugar, se presenta un análisis de las características, estándares, arquitectura y dispositivos de las redes 802.11. Para posteriormente identificar los diferentes riesgos y tipos de ataques informáticos a los cuales se encuentran expuestos estas redes.

Así también se identifican los diferentes mecanismos de seguridad existentes que introducen niveles básicos y avanzados de seguridad en las redes inalámbricas. Se identifica que una herramienta muy empleada para la detección de intrusiones son los llamados sistemas de detección de intrusos inalámbricos (WIDS). Los sistemas de detección de intrusos inalámbricos realizan el análisis de la información que es registrada en las bitácoras del sistema operativo o en el contenido de los paquetes de red, buscando detectar anomalías o abusos realizados por una persona que desee penetrar a un sistema sin previa autorización de su propietario. En este proyecto de tesis se presentará la definición de un sistema de detección de intrusos inalámbrico, sus configuraciones y taxonomía.

Posteriormente se identifican las principales técnicas de detección de intrusiones que son las técnicas basados en uso indebido y en anomalías, se realiza el estudio de los métodos que pueden ser empleados en cada una de estas técnicas. Además se recopila información significativa y actualizada de diferentes artículos académicos desarrollados para la detección de intrusiones en redes 802.11