Universidad Nacional del Litoral

Proyecto Final de Carrera

Diseño de un sistema de detección de anomalías en redes de computadoras.

Informe de avance 1

Pineda Leandro

dirigido por Ing. Miguel Angel Robledo
codirigido por Ing. Gabriel Filippa

Santa Fe
6 de octubre de 2016

Resumen

El presente documento muestra los resultados obtenidos de la etapa de investigación del proyecto final de carrera de Ingeniería en Informática. En primer lugar se mostrará un análisis sobre el modelado del problema y los distintos métodos existentes para la detección de anomalías. Luego se describirán las tecnologías a utilizar, la arquitectura del sistema y sus componentes. Finalmente se dará una breve descripción de las técnicas de modelado a utilizar para detectar anomalías en el tráfico de red.

Introducción

El tráfico de red puede ser caracterizado por la información disponible en la cabecera de los paquetes. El modelo TCP/IP establece que los host deben soportar como mínimo los protocolos IP, ICMP, TCP y UDP[1]. Estos tienen en común dirección de origen y destino: en capa de red se utilizan direcciones IP[2] y en capa de transporte se utilizan puertos[3][4]. Podemos identificar entonces un flujo IP entre dos *host* por una tupla de 5 valores, los cuales forman un espacio de 2^{104} características:

$$\langle IP\ de\ origen,\ IP\ de\ destino,\ puerto\ de\ origen,\ puerto\ de\ destino,\ protocolo \rangle$$

Bibliografía

[1] R Braden, *RFC 1122 Requirements for Internet Hosts - Communication Layers*, 1989. dirección: `http://tools.ietf.org/html/rfc1122`.

[2] J. Postel, ed., *Rfc 791 internet protocol - darpa inernet programm, protocol specification*, Internet Engineering Task Force, 1981. dirección: `http://tools.ietf.org/html/rfc791`.

[3] J. Postel, *User Datagram Protocol*, RFC 768 (Standard), Internet Engineering Task Force, 1980. dirección: `http://www.ietf.org/rfc/rfc768.txt`.

[4] ——, *Transmission Control Protocol*, RFC 793 (Standard), Updated by RFCs 1122, 3168, Internet Engineering Task Force, sep. de 1981. dirección: `http://www.ietf.org/rfc/rfc793.txt`.