Índice

1 Introducción 1

1.1 Definición del problema 4

1.2 Revisión del estado del arte 5

1.3 Objetivo general 10

1.3.1 Objetivos específicos 10

1.4 Contribución 10

1.5 Alcances y limitaciones 11

1.6 Organización de la tesis 13

2 Marco Teórico 15

2.1 IDS (Intrusion Detection Systems) 15

2.1.1 Características 15

2.2 Tipos de IDS 17

2.2.1 Clasificación de los IDS en cuanto a tipos de ataques y utilización de recursos 18

2.2.2 Clasificación de los IDS en cuanto a la metodología de detección de intrusos 19

2.2.3 Clasificación de los IDS en cuanto a lugar y sistemas a monitorizar 20

2.2.4 IPS ("INTRUSION PREVENTION SYSTEMS") 23

2.3 Arquitecturas de los IDS 24

2.3.1 Componentes de los IDS 24

2.3.2 Tipos de arquitecturas de los IDS 24

2.4 Escenarios compatibles para la instalación de un IDS 26

2.4.1 Redes compartidas – Conexión a internet por medio de un Hub 26

2.4.2 Redes conmutadas – Switches con funciones de administración (espejeo de puertos (port mirrioring)) 26

2.4.3 Redes conmutadas – Switches sin funciones de administración (sin espejeo de puertos (no port mirrioring)) 27

2.4.4 Servidor Proxy para compartir Internet 28

2.5 Ataques informáticos 30

2.5.1 Tipos de ataques 30

2.5.2 Desarrollo de los ataques 37

2.7 Discusión 44

3 Modelado y desarrollo 45

3.1 Elementos a utilizar en el diseño, modelado y desarrollo 45
3.1.1 A cerca de Microsoft Visual C# 2008 45
3.1.2 SharpPcap 45
3.1.3 Reglas de Snort 46
3.2 Modelando el IDS UDLA 49
3.2.1 Cargar a memoria las reglas de Snort. 51
3.2.2 División de las reglas para crear grupos. 51
3.2.3 Creación de una tabla mediante el algoritmo de Aho-Corasick. 51
3.2.4 Obtención de la lista de dispositivos 56
3.2.5 Apertura de un adaptador. 56
3.2.6 Captura de paquetes. 57
3.2.7 División de paquetes de acuerdo a su protocolo. 58
3.2.8 Reensamblado de paquetes. 58
3.2.9 Normalización de paquetes. 59
3.2.10 Creación de una tabla de datos que despliega los paquetes capturados. 59
3.2.11 Comparación de paquetes con la tabla creada por el algoritmo Aho-Corasick. 59
3.2.12 Envío de resultados a la tabla de datos. 61
3.2.13 Envío de alertas a la ventana de resumen. 61
3.3 Diseño preliminar de la ventana de salida 61
3.4 Discusión 62
4 Resultados comparativos 63
4.1 Sax2 Network Intrusion Detection System 63
4.1.1 Detección de intrusiones con Ax3soft Sax2 63
4.2 SNORT 64
4.2.1 Análisis de registros IDS con BASE 66
4.3 Pruebas de desempeño de cada uno de los IDS 67
4.3.1 Escenario para las pruebas 67
4.3.2 Desarrollo de las pruebas 68
4.3.3 Comparación y evaluación de resultados 75
4.3.4 Resolución de problemas con Falsos Positivos y Falsos Negativos 78
4.4 Recomendaciones para el diseño de un IDS 80

4.5 Discusión 81

5 Conclusiones y trabajo a futuro 83

5.1 Conclusiones 83

5.2 Trabajo a futuro 84

Bibliografía 87

Apéndice A – Manual de instalación y uso de IDS-UDLAP 95

A.1 Instalación de IDS-UDLA 95

A.1.1 Instalación de .net Framework 3.5 95

A.1.2 Instalación librería de Winpcap 98

A.2 Pasos a seguir para la puesta en marcha del sistema 100

Apéndice B - Programación del IDS 105

B.1 Programación del IDS 105

B.1.1 Cargar a memoria las reglas de Snort 105

B.1.2 División de las reglas para crear grupos 106

B.1.3 Creación de una tabla mediante el algoritmo de Aho-Corasick 106

B.1.4 Obtención de la lista de dispositivos 109

B.1.5 Apertura de un adaptador 110

B.1.6 Captura de paquetes 110

B.1.7 División de paquetes de acuerdo a su protocolo 111

B.1.8 Reensamblado de segmentos TCP 111

B.1.9 Normalización de paquetes 114

B.1.10 Creación de una tabla de datos que despliega los paquetes capturados 116

B.1.11 Comparación de paquetes con la tabla creada por el algoritmo Aho-Corasick 118

B.1.12 Envío de resultados a la tabla de datos 120

B.1.13 Envío de alertas a la ventana de resumen 120