

ÍNDICE DE CONTENIDO

Página.

| | |
|---|------------|
| DEDICATORIA..... | i |
| RESUMEN..... | ii |
| ÍNDICE DE CONTENIDO | iv |
| ÍNDICE DE FIGURAS. | vii |
| ÍNDICE DE TABLAS. | x |
| | |
| CAPITULO 1. INTRODUCCIÓN..... | 1 |
| 1.1 Antecedentes..... | 1 |
| 1.2 Planteamiento del Problema | 6 |
| 1.3 Objetivo de la Tesis | 6 |
| 1.4 Organización de la Tesis | 7 |
| | |
| CAPITULO 2. SISTEMAS DE DETECCIÓN DE INTRUSOS | 9 |
| 2.1 Intrusos y Ataques en la Red | 9 |
| 2.1.1 Ataque Pasivo | 11 |
| 2.1.2 Ataque Activo | 11 |
| | |
| 2.2 Sistemas para Detección de Intrusos | 12 |
| 2.2.1 Clasificación de los IDS | 13 |
| 2.2.2 Colocación de un IDS en la Red | 14 |
| | |
| 2.3 Snort Rule de un IDS | 16 |
| 2.4 Implantación de las Barreras de Protección | 18 |
| 2.5 Firewall..... | 19 |
| 2.6 IPS (Intuder Prevention System)..... | 21 |
| 2.7 Políticas de Seguridad en Redes..... | 23 |
| 2.8 Discusión..... | 23 |
| | |
| CAPITULO 3. OMNET++ | 24 |
| 3.1 Descripción de OMNET++ | 24 |
| 3.1.1 Elementos de simulación de OMNET++ | 25 |
| 3.1.2 Lenguaje NED y Ambiente GNED..... | 26 |
| 3.1.3 Lenguaje C++ | 27 |
| 3.1.4 Ambiente de Simulación TKENV | 27 |

| | |
|---|-----------|
| 3.1.5 Herramientas de Graficación Histogram, Vector y Scalars | 28 |
| 3.2 Programas Alternativos para la Simulación de Redes | 30 |
| 3.2.1 Packet Tracer..... | 30 |
| 3.2.2 NCTUns 2.0 Network Simulator/ Emulator..... | 31 |
| 3.2.3 OPNET..... | 31 |
| 3.3 Discusión..... | 33 |
| | |
| CAPITULO 4. DISEÑO DEL IDS..... | 34 |
| 4.1 Topología de Red | 37 |
| 4.2 Zona Desmilitarizada (DMZ)..... | 37 |
| 4.3 Ataques Implementados para la Simulación | 37 |
| 4.3.1 DoS (Denial Of Service)..... | 38 |
| 4.3.2 DDoS (Distributed Denial of Service)..... | 39 |
| 4.3.3 Ping of Death..... | 40 |
| 4.3.4 XSS (<i>Cross-Site Scripting</i>) | 40 |
| 4.3.5 Ataque MITM (<i>Man in the Middle</i>)..... | 41 |
| | |
| 4.4 Snort Rule del IDS diseñado | 42 |
| 4.5 Discusión | 44 |
| | |
| CAPITULO 5. IMPLEMENTACIÓN DEL IDS EN OMNET++..... | 45 |
| 5.1 Presentación del tráfico y Ataques en la Red..... | 45 |
| 5.1.1 Mensajes en el tráfico de Red..... | 45 |
| 5.1.2 Generación de Ataques sobre la Red..... | 48 |
| | |
| 5.2 Diseño e Implementación del IDS | 49 |
| 5.2.1 Diseño e Implementación del Firewall..... | 51 |
| | |
| 5.3 Discusión..... | 52 |
| | |
| CAPITULO 6. PRUEBAS Y RESULTADOS..... | 53 |
| 6.1 Introducción..... | 53 |
| 6.2 Ataque DoS | 55 |
| 6.3 Ataque DDoS..... | 58 |
| 6.4 Ataque PoD | 63 |
| 6.5 Ataque XSS..... | 67 |
| 6.6 Ataque MiTM..... | 71 |
| 6.7 Pruebas y Desempeño del IDS diseñado..... | 72 |
| 6.7.1 Falsos negativos y Falsos Positivos..... | 80 |

| | |
|--|-----------|
| 6.8 Discusión..... | 84 |
| CAPITULO 7. CONCLUSIONES Y TRABAJO A FUTURO..... | 85 |
| 7.1 Conclusiones | 85 |
| 7.2 Trabajo a Futuro | 86 |
| APÉNDICEA..... | 87 |
| APÉNDICE B. CÓDIGO DE IMPLEMENTACIÓN DE LOS ATAQUES EN OMNET++..... | 88 |
| BIBLIOGRAFÍA..... | 93 |