CAPITULO 6

PRUEBAS Y RESULTADOS

Concluidas la programación y las simulaciones se obtuvieron resultados acerca de los eventos ocurridos durante las simulaciones en *OMNET++*. Con base en estos datos se analizó el comportamiento que se tuvo en la red para así comparar el resultado obtenido por cada esquema de ataque simulado y posteriormente comprobar la efectividad del diseño para el IDS. También se expone la implementación de los ataques que se utilizaron para la simulación ofreciendo al usuario un resultado que le permita comprender de manera analítica el comportamiento de una red en cuanto al aspecto de seguridad.

6.1 Introducción

Una vez establecida la topología de red con sus características y el tráfico, el siguiente proceso fue realizar pruebas por medio de la implementación de los ataques mencionados en el capítulo 2 para obtener resultados que permitieran medir el desempeño del IDS diseñado en base a las gráficas obtenidas con las herramientas de programación que OMNET++ proporciona. Para realizar la simulación se consideraron factores que pueden ser programados y variados para obtener y comparar los diferentes resultados de las simulaciones, todo esto a través de la ventana *OMNETini* (véase la Figura 6.1)

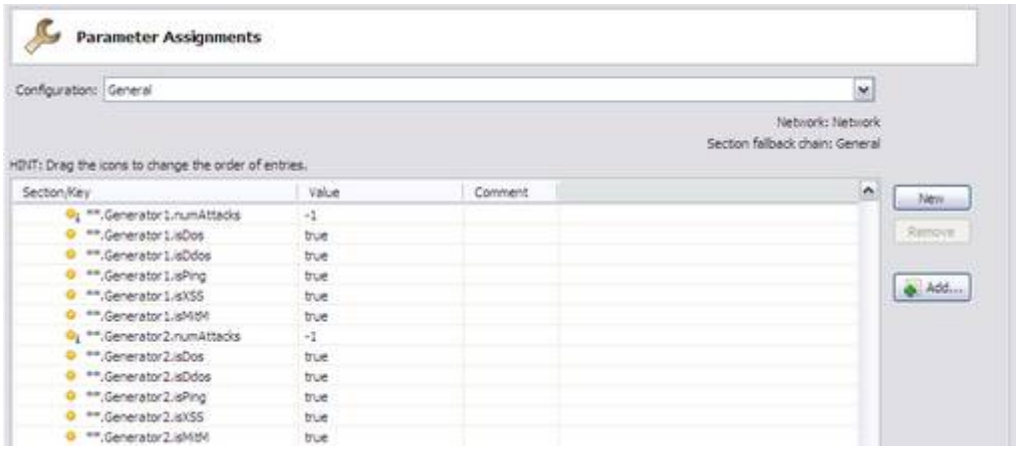


Figura 6.1: Establecimiento de los parámetros para la simulación, ventana *OMNETini.*

En la Figura 6.1 la ventana *OMNETini* permite la activación de los intrusos y los ataques que serán generados en el tráfico.

Una vez establecidos los parámetros se realizaron las pruebas y observación de los resultados obtenidos. A continuación se presentan dichas pruebas y cuyo primer bloque consistió en observar cómo los ataques afectaban el ancho de banda de los nodos PCs y Servidores. El análisis se realizará de manera separada para cada ataque, después con todos los ataques activados y por último con la activación de los IDS para verificar su desempeño.

Los resultados obtenidos fueron en función de una generación de ataques en un intervalo de tiempo de 0.20 segundos tanto para el *Generador 1 y 2 de ataques*, con un retardo de propagación en los enlaces de comunicación (los contactos entre los nodos) de 120 ms (milisegundos). Estos tiempos fueron establecidos considerándose un modelo de red LAN en el que los enlaces de comunicación tienen una velocidad de propagación de $2x10^8 m/s$, ya que son cables de red cuyo material es cobre y en el que cada paquete o mensaje generado sobre la red simulada tiene un tamaño de 6 Mb(Megabits). Siendo así que el retardo de propagación se obtiene de la siguiente manera:

$$\text{Re}\,tardo\ de\ propagación = \frac{L}{R}, L\ es\ el\ tamaño\ del\ paquete\ y\ R\ la\ tasa\ de\ transferencia\ del\ enlace.$$

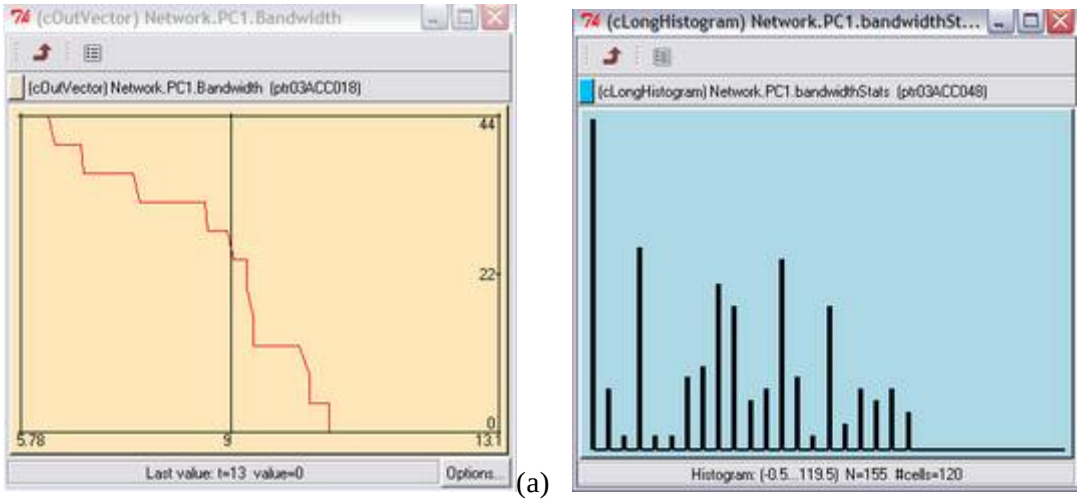
$$\text{Re}\,tardo\ de\ propagación = \frac{6Mb}{50Mbps} = 120ms, donde\ b\ son\ bits\ y\ Mbps\ Megabits\ por\ segundo.$$

[54]

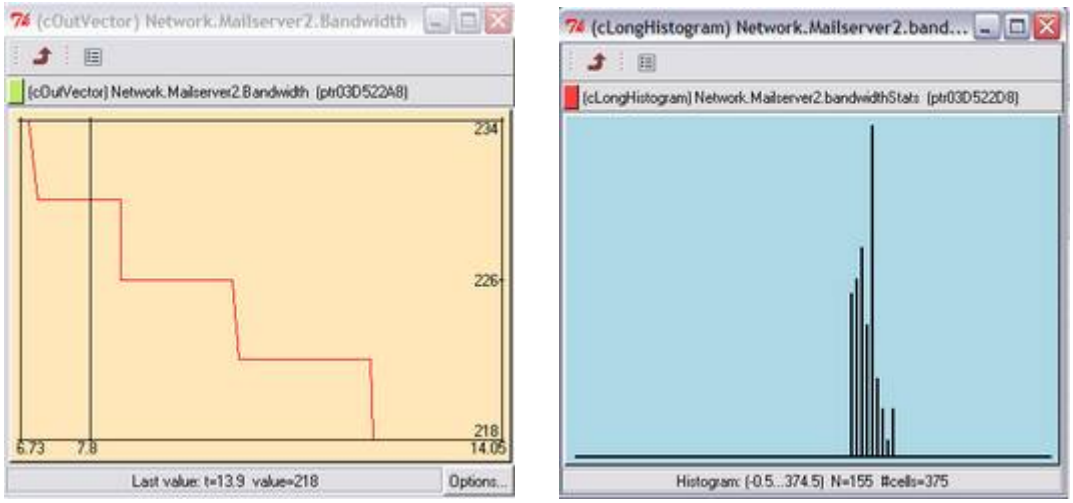
Por otra parte el tiempo de generación establecido para el tráfico compuesto por los paquetes o datos y ataques se consideró con el valor antes mencionado de manera que su generación en la simulación permita que los paquetes puedan distribuirse en la red para que al llegar a los nodos se pueda observar la detección y el efecto del tráfico en los elementos de la red evitando así un retardo de cola en el cual la tasa de llegada es mayor que la tasa de servicio o procesamiento. De esta manera el tiempo de generación es poco menor que el doble del retardo de transmisión.

6.2 Ataque DoS

El ataque *DoS* es un ataque de denegación de servicio cuyo desempeño se muestra con el consumo del BW. En la simulación este ataque puede provocar tal daño a este recurso en cualquiera de las PCs o servidores sobre la red. Para la sección de los ataques se emplearon las herramientas *Vector* e *Histogram* que muestra la caída del ancho de banda de los nodos PC1 (a) y MailServer2 (b), tomados como ejemplo (véase la Figura 6.2).



(a)



(b)

Figura 6.2: Consumo del BW del MailServer2 y PC1 causado por ataque DoS. Se utilizan herramientas de programación: *Vector* e *Histogram*.

Para la simulación de los ataques el BW establecido como recurso para la PC1 fue de 80 Mbps mientras para los servidores tal como el MailServer 2 fue de 250 Mbps. En la Figura 6.2 (a) se observa como el BW de la PC1 decrementa a una tasa de 22 Mbps, mientras que en la Figura 6.2 (b) el BW del MailServer2 se reduce a una tasa de 16 Mbps. Cabe mencionar que la tasa de decremento es aleatoria y no se puede fijar.

En las gráficas mostradas en la Figura 6.2 el ancho de banda (*BW*) se refleja en el eje Y y el tiempo (en segundos) en el eje X.

A continuación se muestran los valores estadísticos registrados durante la ejecución de la simulación. Primero se muestra el comportamiento del BW de los servidores y PCs afectadas, (véanse las Figuras 6.3 y 6.4).

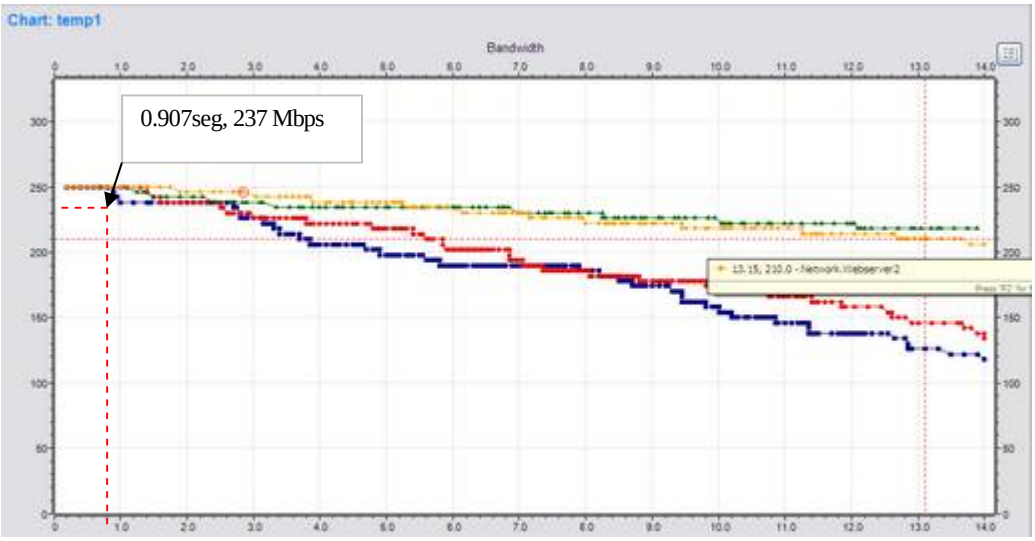


Figura 6.3: Comportamiento del BW de los Servidores afectados por el ataque DoS. Mail Server 2 (verde), Web Server 2 (amarillo), Web Server 1(rojo) y Mail Server 1 (Azul).

Web Server 2 y Mail Server 2 están colocados en la *DMZ* o Zona Desmilitarizada. La ventana amarilla mostrada en la Figura 6.3 aparece al dar click sobre la gráfica deseada, mostrando en ese punto el tiempo en segundos y el valor del BW en Mbps.

En este caso en la simulación, el primer elemento afectado en la red por el ataque fue el MailServer1 a los 0.907 segundos de haber sido ejecutada la simulación, reduciéndose el

valor del BW a 238 Mbps. A continuación para los nodos PC se capturó la siguiente información respecto al BW (véase la Figura 6.4).

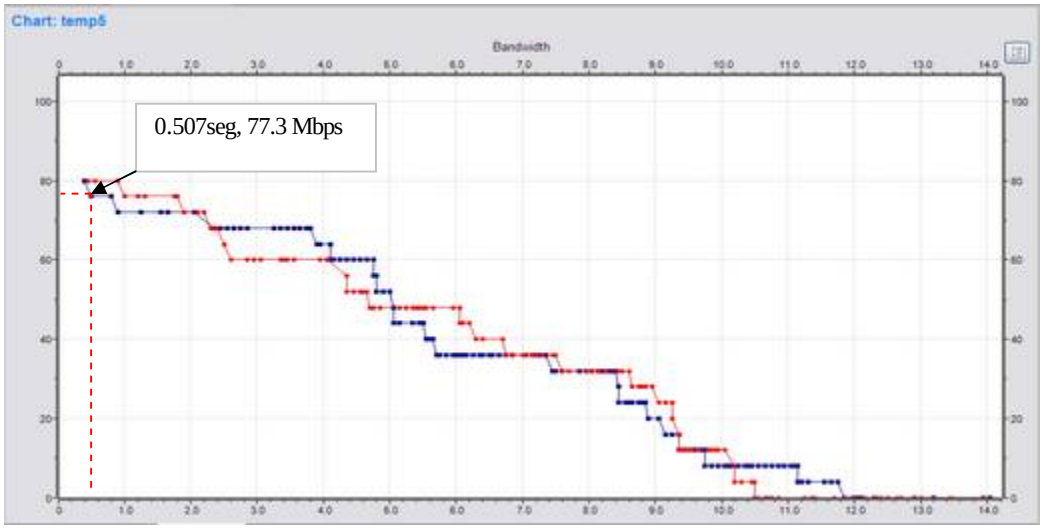


Figura 6.4: Comportamiento del BW de las PCs afectadas por el ataque DoS. PC1 (rojo) y PC3 (Azul).

Tal como se muestra en la Figura 6.4. La PC 3 fue el primer elemento afectado por el ataque, en un tiempo de 0.507 segundos de haber comenzado la simulación y reducir a 77.3 Mbps el BW. Cada mensaje detectado como amenaza *DoS* provocaba el decremento del mismo recurso y cuyo valor fue de los 80 Mbps establecidos inicialmente, reduciendo su valor a 60 Mbps a los 4.8 segundos y finalmente cayendo el ancho de banda a 0 Mbps del mismo nodo a los 11.7 segundos.

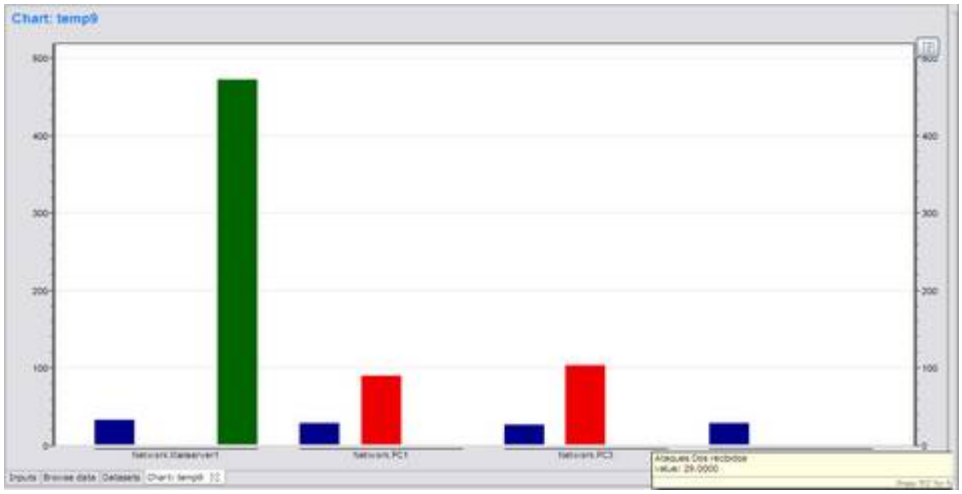


Figura 6.5: Estadísticas del tráfico detectado por los Servidores y PCs.

A continuación se obtuvo el registro del tráfico detectado por los siguientes elementos: MailServer1, PCs 1 y 3 y el WebServer1 (véase la Figura 6.5). La gráfica Azul muestra los ataques DoS detectados mientras que las barras verde y rojas indican los mensajes *Data* registrados. De la misma manera para conocer el valor del registro basta con dar click en la barra. Esta gráfica se obtuvo por medio de la herramienta *Scalars*. En la misma figura se muestra que en el periodo que duró la simulación se detectaron los siguientes paquetes, registrados en la Tabla 6.1.

Tabla 6.1. Paquetes registrados durante el ataque DoS.

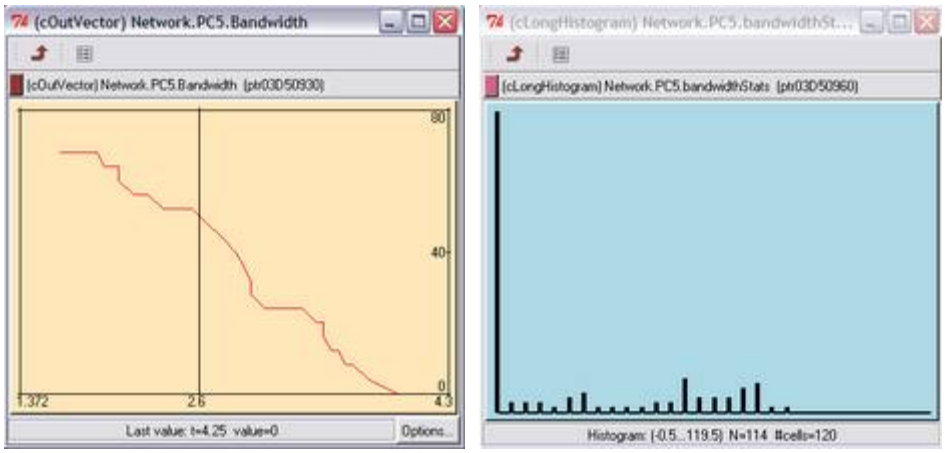
Elementos de la Red	**Datos**	**Ataques DoS**	
WebServer1	475	43	
MailServer1	0	33	
PC1	90	28	
PC3	103	26	**Paquetes totales**
Total	**668**	**160**	**828**

La Tabla 6.1 muestra los valores de los datos y ataques DoS registrados en un intervalo de tiempo de 14.3 segundos en la simulación. Durante ese periodo de tiempo se detectaron 668 datos y 160 ataques DoS, dando un total de 828 paquetes detectados.

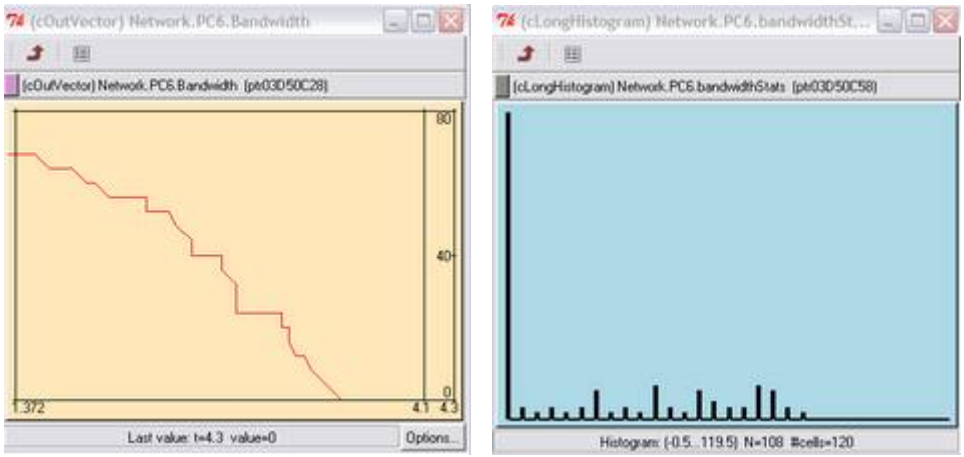
6.3 Ataque DDoS

El ataque *DDoS* también considerado como un ataque de denegación de servicio actúa como una amenaza que provoca daño al BW en cualquiera de las PCs sobre la red de la simulación, las cuales distribuirán el ataque DoS hacia una víctima en específico en la red, tal como se muestra a continuación (*bots*).

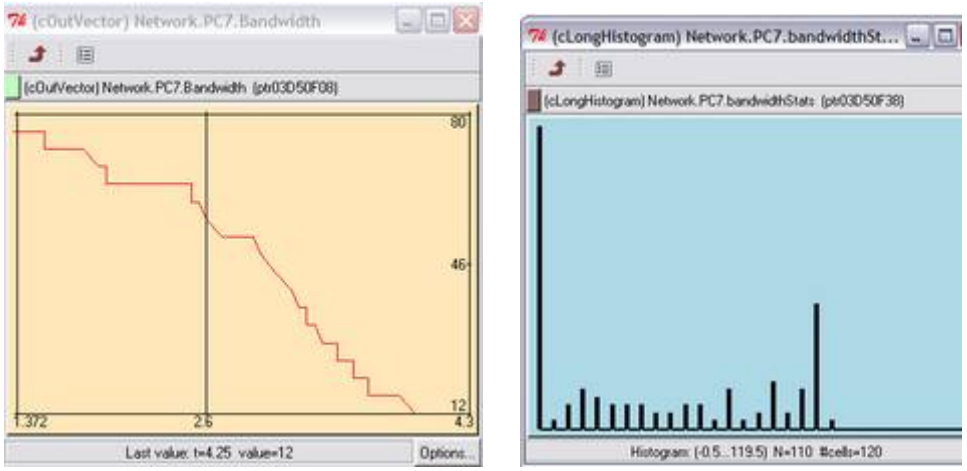
En este ataque los resultados se enfocan en la subred con las PCs 5, 6 y 7, puesto que en la misma se encuentra el Generador de ataques 2 y que por lo tanto es el que genera dicho ataque que afectó directamente a los elementos PC mencionados (véase la Figura 6.6).



(a)



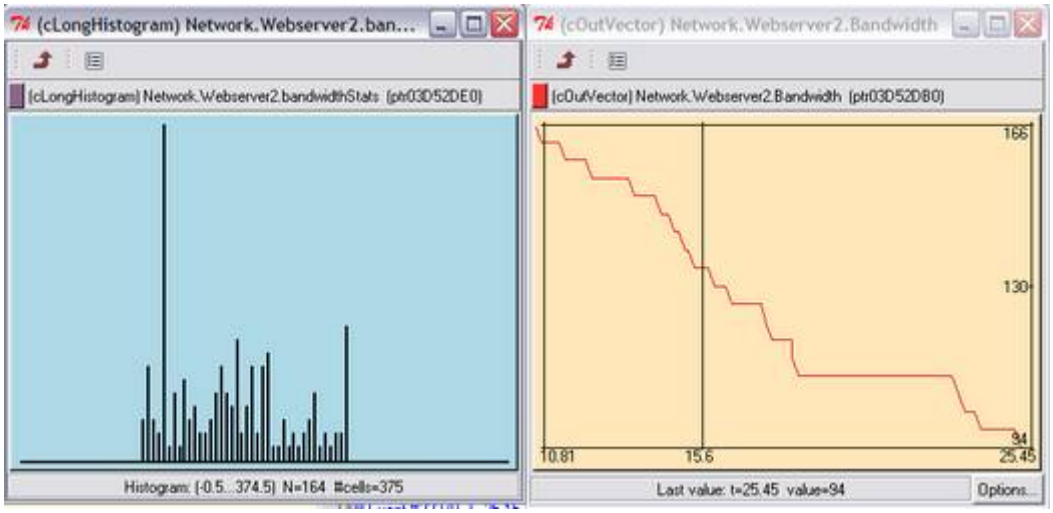
(b)



(c)

Figura 6.6: Variación del BW de los nodos afectados por el ataque DDoS. Puntos de la red afectados (a) PC5, (b) PC6 y (c) PC7.

Dado el tipo de ataque se analizó el comportamiento del BW del WebServer2 ubicado en la *DMZ*. En la simulación se muestra que tanto las PCS 5, 6 y 7 como el servidor mencionado fueron afectados por este ataque mostrados en los mensajes de la red simulada (véanse las Figuras 6.7 y 6.8).



(a) (b)

Figura 6.7: Respuesta del BW del WebServer2 afectado por el ataque DDoS.

En la gráfica del histograma (a) del WebServer2 se muestra cómo a mayor cantidad de paquetes DDoS recibidos el BW se colapsa a 246.3 Mbps en un periodo de tiempo (2.4 segundos), puesto que sobre este nodo actúan las PCs controladas.

Comparando este ataque con el anterior el MailServer2 afectado por el ***DoS*** decrementó su BW a 218 Mbps en aproximadamente 13.5 segundos (véase la Figura 6.3), mientras que por otra parte, en ese intervalo de tiempo el WebServer2 tenía el nivel de su Bw a 150 Mbps, afectado por el ataque ***DDoS*** (véase Figura 6.7 (b)).

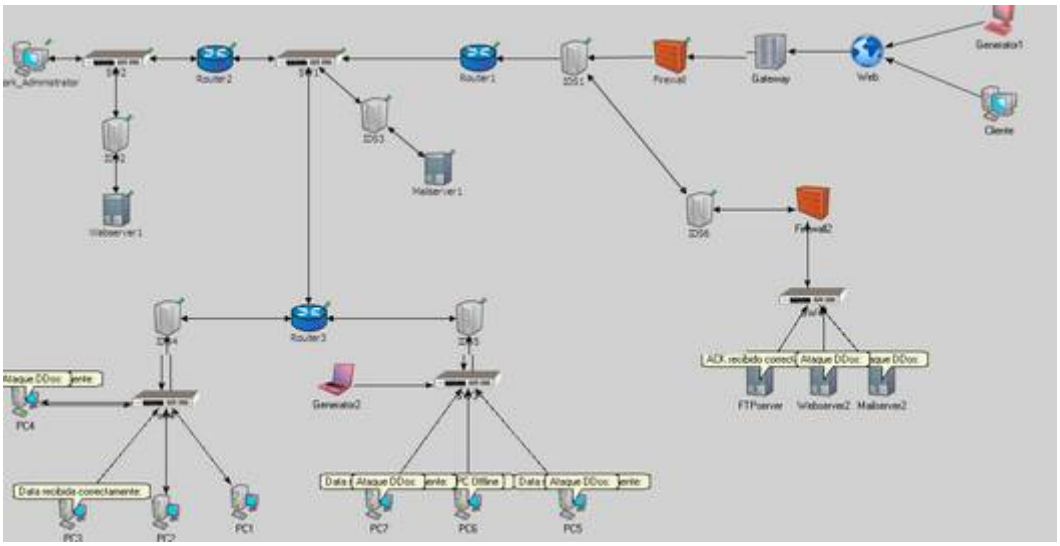


Figura 6.8: Simulación corrida sobre la red. Se muestra el ataque DDoS sobre los nodos afectados.

A continuación se muestran los valores estadísticos registrados durante la ejecución de la simulación durante el ataque DDoS. En la Figura 6.9 se muestra el comportamiento del BW para las PCs afectadas por el ataque. Tal como se puede observar el BW de cada equipo se colapsa de manera similar ya que se distribuyó el ataque en las PCs ya mencionadas. Se indica la correspondencia de cada gráfica con su respectivo elemento de la red en la misma figura.

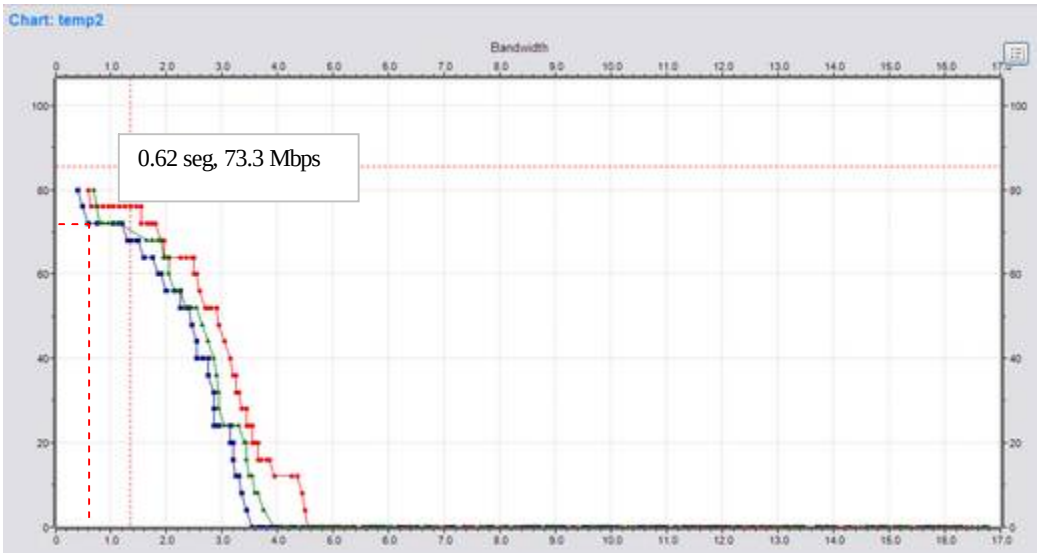


Figura 6.9: Comportamiento del BW de las PCs afectadas por ataque DDoS. PC5 (verde), PC6 (azul) y PC7 (rojo).

Posteriormente se presenta el comportamiento del Bw, tanto del WebServer2 como del MailServer2, los cuales fueron los afectados por el ataque DDoS.

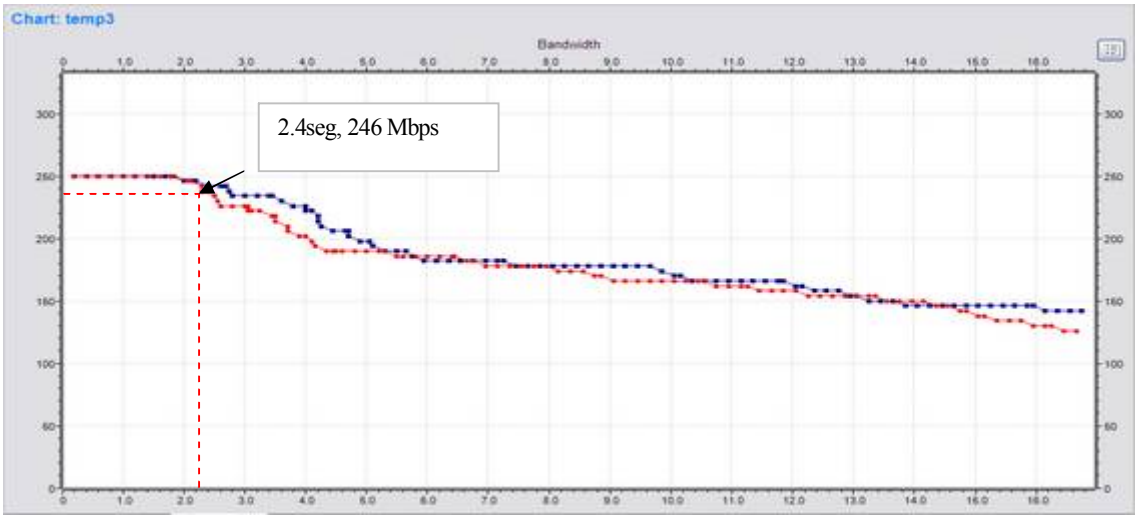


Figura 6.10: Comportamiento del BW del MailServer2 (azul) y WebServer2 (rojo).

La Figura 6.10 presenta el comportamiento del BW con respecto al ataque DDoS, de la misma manera en comparación con el ataque *DoS* de la sección anterior, los mismos servidores se encontraban con un BW por apenas debajo de los 200 Mbps a los 14 segundos de la simulación, mientras que ante el *DDoS* los servidores ya tenían un BW disponible de apenas 150 Mbps. Debido a que el atacante genera un gran flujo de información desde varios puntos de conexión en contra de la "víctima".

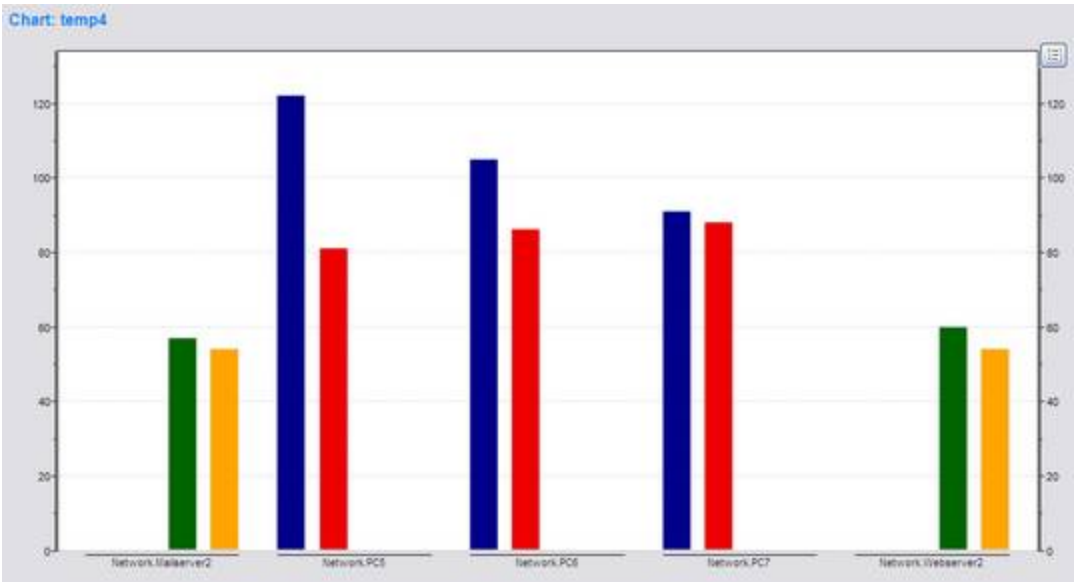


Figura 6.11: Estadísticas del tráfico detectado por los Servidores y PCs.

Se registró el tráfico detectado por los siguientes elementos: MailServer2, PCs 5, 6 y 7, y el WebServer2 (véase la Figura 6.11). La gráfica Azul muestra los ataques DDoS detectados mientras que las barras verde y rojas indican los mensajes *Data* registrados. A continuación en la Tabla 6.2 se presentan los valores registrados.

Tabla 6.2. Paquetes registrados durante el ataque DDoS.

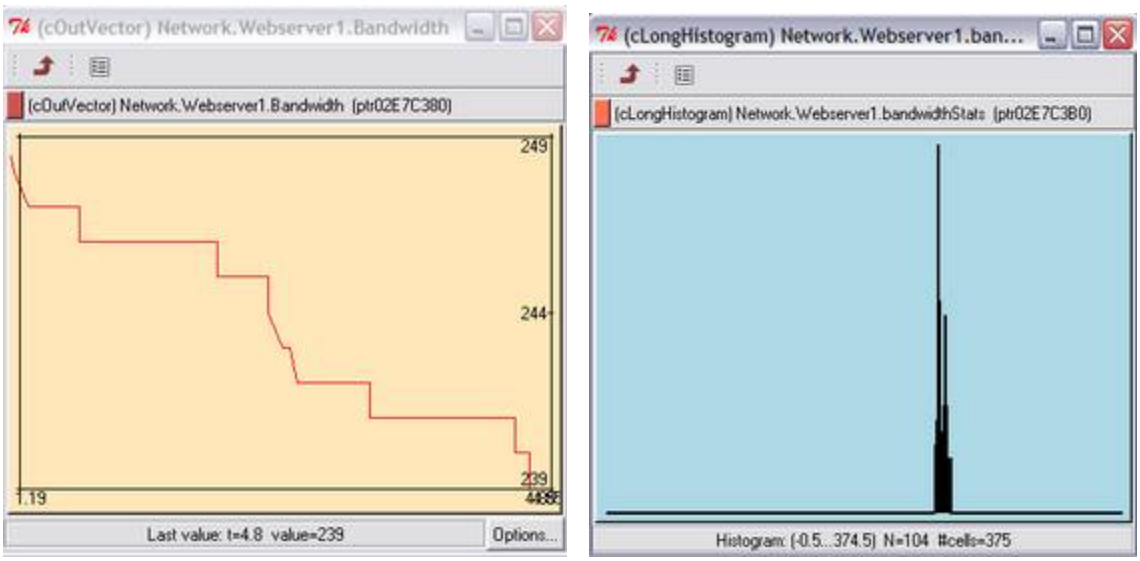
Elementos de la Red	**Datos**	**Ataques DDoS**	
WebServer2	60	54	
MailServer2	57	54	
PC5	81	122	
PC6	86	105	
PC7	91	88	**Paquetes totales**
Total	**375**	**423**	**798**

La Tabla 6.2 contiene el registro de los datos y ataques que formaron parte del tráfico para esta simulación en el que tanto MailServer2 como WebServer2 recibieron la misma cantidad de ataques, siendo así que casi de manera síncrona se veía afectado su BW y de manera proporcional (Véase la figura 6.10).

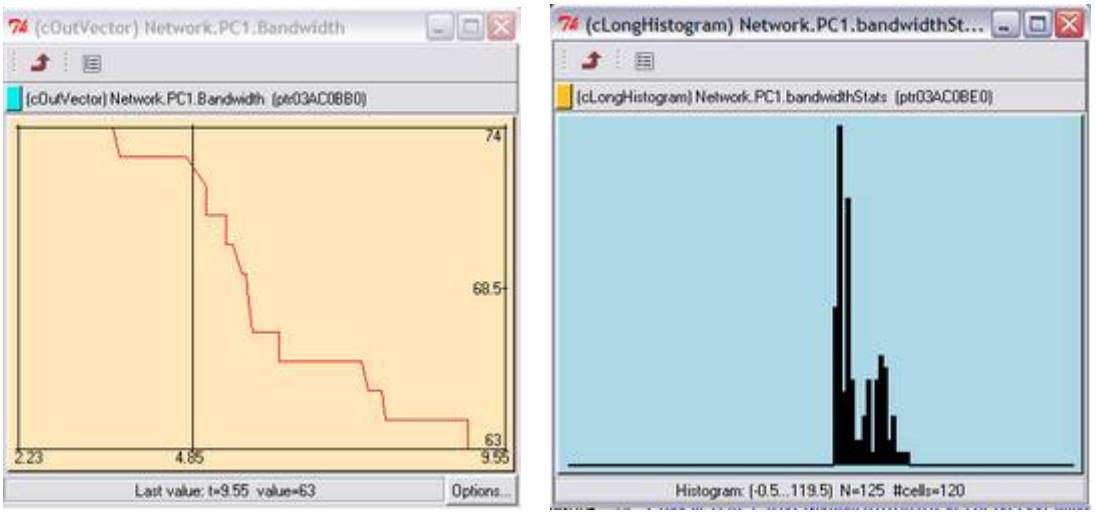
En esta tabla se presentan los datos y ataques DDoS registrados en un intervalo de tiempo de 17 segundos de la simulación. Durante ese periodo de tiempo se detectaron 375 datos y 423 ataques DDoS dando un total de 798 paquetes registrados en los elementos presentes en la misma tabla.

6.3 Ataque PoD (*Ping of Death)*

Como se describe en el capítulo 2 un PoD es un ataque enviado a una computadora o servidor, el cual consiste en enviar numerosos paquetes ICMP pesados mayores a 65.535 bytes con el fin de colapsar el BW del sistema atacado. Los resultados que a continuaciones mostrarán reflejan en las PCs y Servidores el daño al BW (véase la figura 6.12).



(a)



(b)

Figura 6.12: Variación del BW de los nodos afectados por el ataque Ping de la muerte. Colapso del Bw de WebServer1 (a) y PC1 (b).

En la Figura 6.12 se muestra el valor del BW del WebServer1 y de PC1, reflejando el colapso de su BW. Los histogramas reflejan la variación del mismo recurso de los elementos seleccionados, tomando como referencia el estado inicial del BW y el cual varía conforme recibe los paquetes *Ping de la muerte* la víctima.

A continuación en la Figura 6.13 se presenta la gráfica del BW del MailServer1 y WebServer1, que en la topología de la red representan ser servidores privados y que fueron los elementos sobre los que se toma el análisis del ataque.

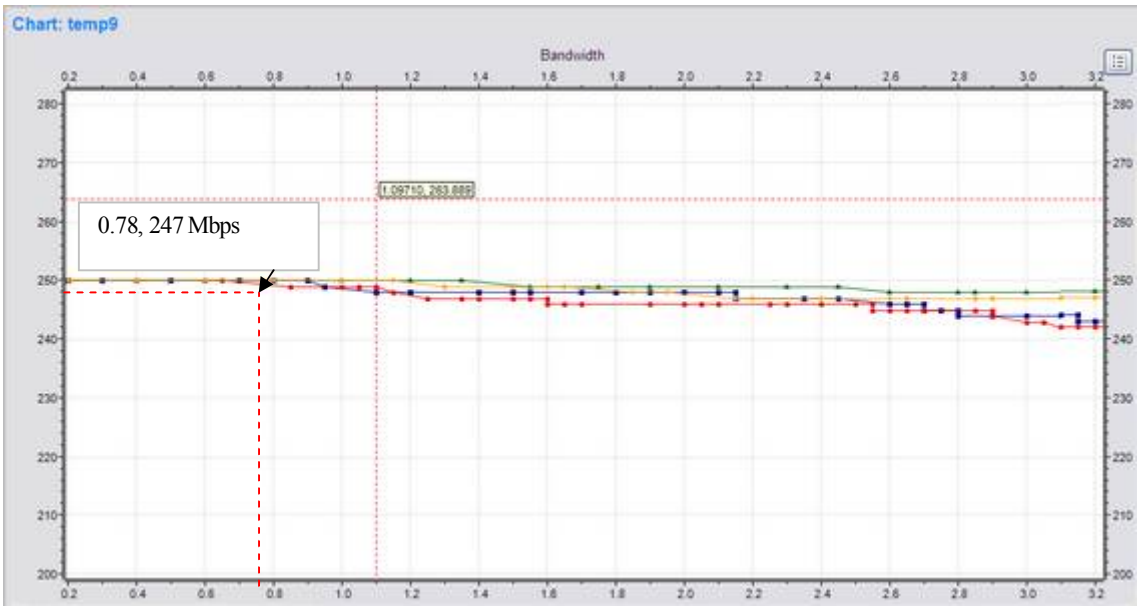


Figura 6.13: Comportamiento del BW del MailServer1 (azul), WebServer1 (rojo), MailServer 2 (verde) y WebServer2 (amarillo).

Las gráficas presentes en la Figura 6.13 reflejan la variación del BW de estos elementos de la red, a comparación de los otros ataques el BW es un recurso que no colapsa tan rápido como ante los otros ataques ocurrió. Por otro lado el BW proporcionado es mucho mayor (250 Mbps) y siendo que el *Ping of Death* se toma como un paquete de 65.535 Bytes y cuyo daño será incrementado de acuerdo a la cantidad de paquetes que entren en los elementos "víctima".

Comenzado el efecto del ataque a los 0.78 segundos después de haber comenzado la simulación y siendo afectado el BW disminuyendo en ese punto del tiempo a 247 Mbps del WebServer1. A continuación se presenta el registro de las máquinas que fueron infectadas por los paquetes del ataque PoD en la simulación.

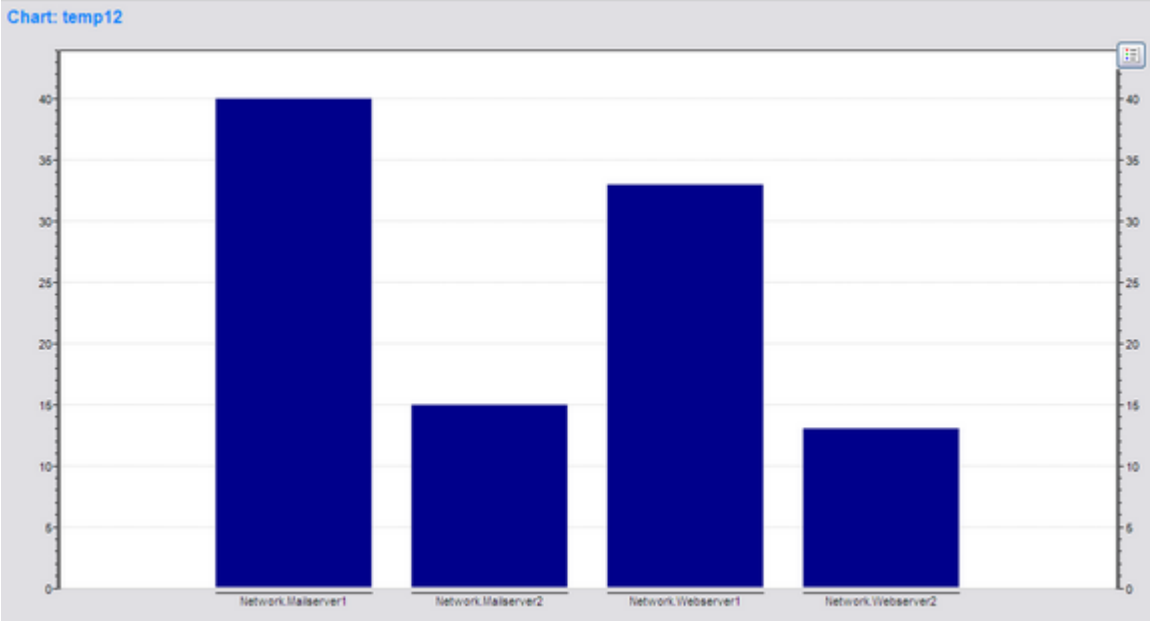


Figura 6.14: Estadísticas de los ataques Ping de la muerte detectado por los Servidores.

En la Figura 6.14 se muestra el registro de los ataques Ping de la muerte detectado por los siguientes elementos: MailServer1 y 2, y los WebServer1 y 2. La gráfica en barras de color azul muestra los ataques detectados.

Tabla 6.3. Valores registrados durante el ataque PoD.

Elementos de la Red	Datos	Paquetes PoD	Variación del Bw
WebServer2	27	13	A los 1.3 segundos decremento a 249 Mbps.
MailServer2	12	15	A los 1.48 segundos decremento a 249 Mbps.
WebServer1	16	33	A los 0.85 segundos decremento a 249 Mbps.
MailServer1	19	40	A los 1.8 segundos decremento a 240 Mbps
Totales	**74**	**101**	
Paquetes totales	**175**		

En la Tabla 6.3 se puede observar que los valores de la variación en el BW para los elementos evaluados es mínimo dicha característica se programó para diferenciar este ataque de los anteriores (*DoS y DDoS*) puesto que también forma parte de los ataques de denegación de servicio pero no es tan complejo como los anteriores**.**

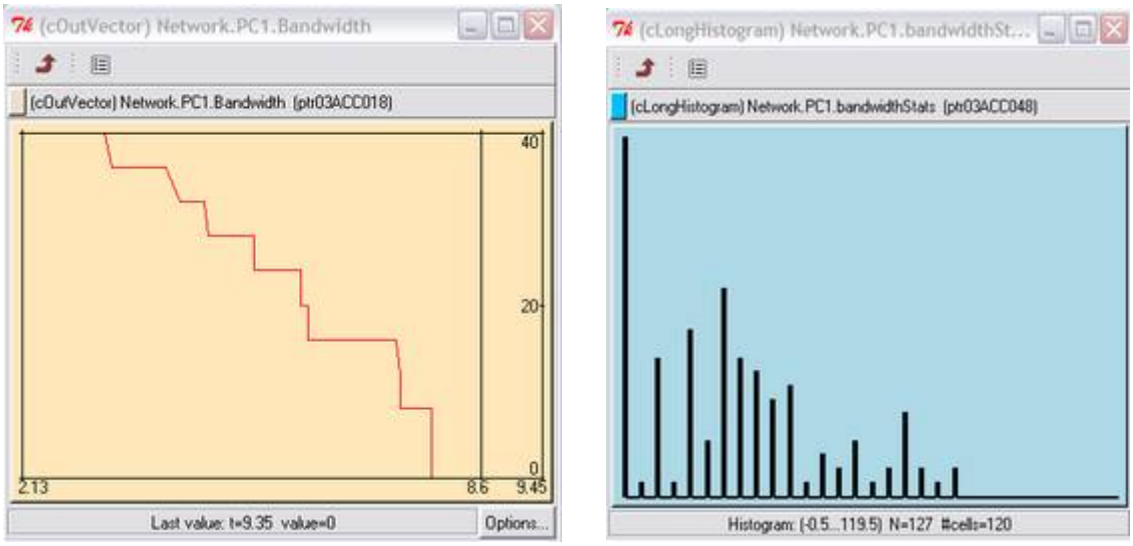
Por otra parte en base al registro del tráfico se detectaron 74 ataques y 102 paquetes PoD dando un total en el tráfico para los elementos analizados de 175 paquetes en un intervalo de tiempo de 4.25 segundos.

6.4 Ataque XSS

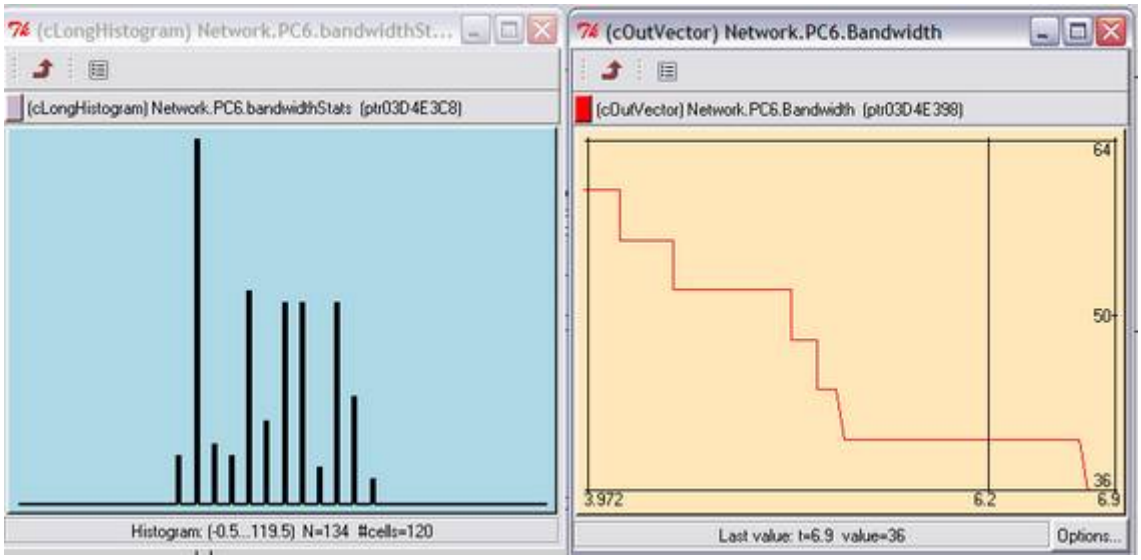
Es un tipo de intrusión que explota la vulnerabilidad del sistema de validación *HTML*. Es un ataque contra aplicaciones Web en los que un atacante toma el control sobre el navegador de un usuario con el objetivo de ejecutar códigos o *scripts* maliciosos escritos en lenguaje HTML o JavaScript.

Debido a que en este trabajo de tesis se presenta como factor de análisis el BW de los elementos de la red, el ataque *XSS* reflejará de la misma manera su desempeño afectando este recurso de tal modo que el colapso provocado en él demuestra que el atacante puede controlarlo a través de sus víctimas (véase la Figura 6.15).

Para este ataque los histogramas muestran de manera más clara la variación del uso del BW de las víctimas, tal como se aprecia en los bloques de la Figura 6.15 (a) y (b). El desempeño de este recurso depende de la cantidad de intrusiones *XSS* ocurridas en la simulación (véase la Figura 6.16).



(a)



(b)

Figura 6.15: Variación del BW de los nodos afectados por el ataque XSS. Colapso del BW de PC1 (a) y PC6 (b).

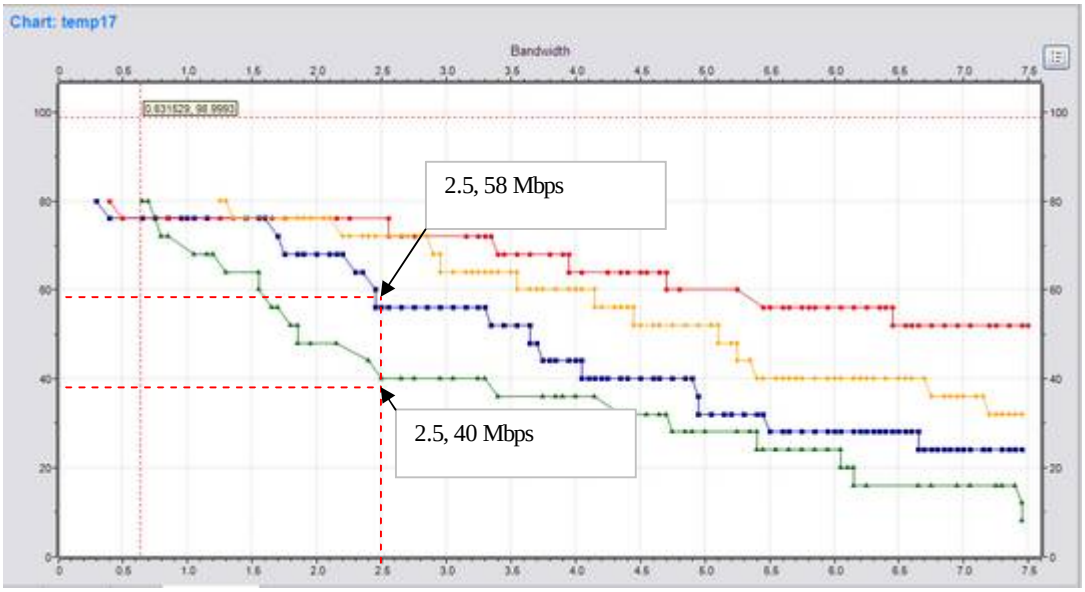


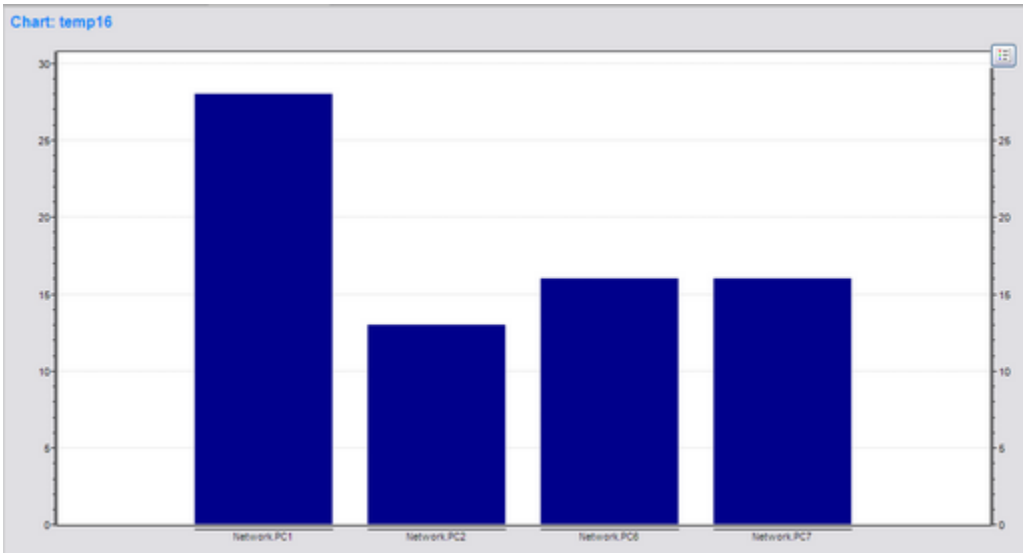
Figura 6.16: Comportamiento del BW de la PC1 (verde), PC2 (rojo), PC6 (amarillo) y PC7 (azul), ante el ataque *XSS*.

Para este ataque se programó que el BW se afectara de tal manera que los resultados de la gráfica mostrarán como se colapsa más rápido este recurso pues la secuencia de los ataques *XSS* en la víctima es la que provoca tal daño. Tal como se puede apreciar el elemento PC1 es la primera en colapsar por completo el BW en un tiempo de 7.88 segundos una vez empezada la simulación.

A los 2.5 segundos de haber sido iniciada la simulación, se registró que el BW de los nodos analizados de la red refleja la mayor afectación obteniendo los siguientes resultados:

- PC1 disminuyó su BW a los 39 Mbps
- PC2 disminuyó su BW a los 76 Mbps
- PC6 disminuyó su BW a los 75 Mbps.
- PC7 disminuyó su BW a los 57 Mbps.

A continuación se presenta el registro de los ataques XSS en las computadoras de la red que fueron víctimas (véase la Figura 6.17).



6.17: Estadísticas de los ataques *XSS* registrados en las víctimas (PC1, (PC2), (PC6), (PC7)).

Establecido el periodo de simulación de 12.5 segundos fueron registrados los siguientes valores de ataques *XSS* en las PCs ya mencionadas en la Tabla 6.4.

Tabla 6.4. Valores registrados durante el ataque XSS.

Elementos de la Red	**Datos**	**Ataques XSS**	
PC1	20	28	
PC2	13	13	
PC6	22	16	
PC7	25	16	**Paquetes totales**
Total	**80**	**73**	**153**

La Tabla 6.4 contiene el registro del tráfico detectado, siendo de 73 ataques XSS y 80 paquetes o datos del tráfico que no afecta el BW dando un total para los elementos analizados de 153 paquetes en un intervalo de tiempo de 12.5 segundos.

6.5 Ataque MiTM

Se caracteriza por ser un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar los mensajes entre dos partes sin que ninguna de ellas conozca que en medio de entre ellos se ha colocado el intruso.

El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas, esto lo hace a través de un *Sniffer*, el cual es un software herramienta que le permite monitorear el tráfico en la red. Dado el desempeño de este ataque se tomo como referencia para el funcionamiento del Firewall, puesto que este sistema se establece como una de las medidas de seguridad o filtro.

El uso de este ataque en este trabajo de tesis se enfoca en hacer uso del Firewall como un medio de seguridad, siendo para los IDS un filtro (véase la Figura 6.18). La acción tomada por parte del Firewall se visualiza a través de un mensaje como *MiTM detenido* indicando que el ataque fue reconocido, detectado y por lo tanto detenido.

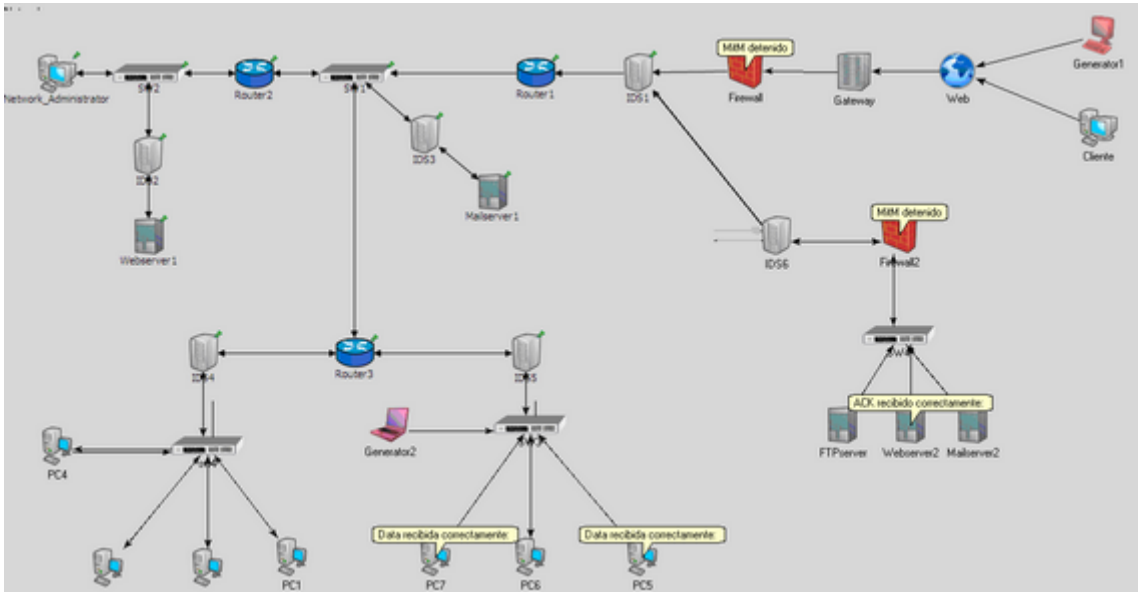


Figura 6.18: Detección del ataque MiTM por el Firewall.

6.6 Pruebas y Desempeño del IDS diseñado

Una vez presentados los ataques y expuestos sus resultados, el siguiente proceso fue realizar el diseño y simulación del IDS para medir su desempeño y saber qué tan eficiente es ante los ataques programados para la simulación. Como parte inicial se llevará acabo la activación de los IDS y se programaron para detectar ciertos ataques, con el propósito de mostrar el funcionamiento en la mayoría de ellos, a través de la ventana *OMNETini* cambiando su estado de *false* a *true.*

La prueba principal consiste en que los generadores crearán todos los ataques explicados anteriormente junto con mensajes y datos, de tal manera que los IDS establecidos sobre la red puedan identificar entre los ataques y el tráfico normal que transita sobre ella.

En primera instancia se mostrarán las gráficas de vector e histogramas de algunos de los nodos de las subredes y en los que se observará que no hay variación en el desempeño del BW de los mismos equipos, es decir que los ataques no provocaron daño alguno en los elementos PCs o servidores de la red (véase la Figura 6.19).

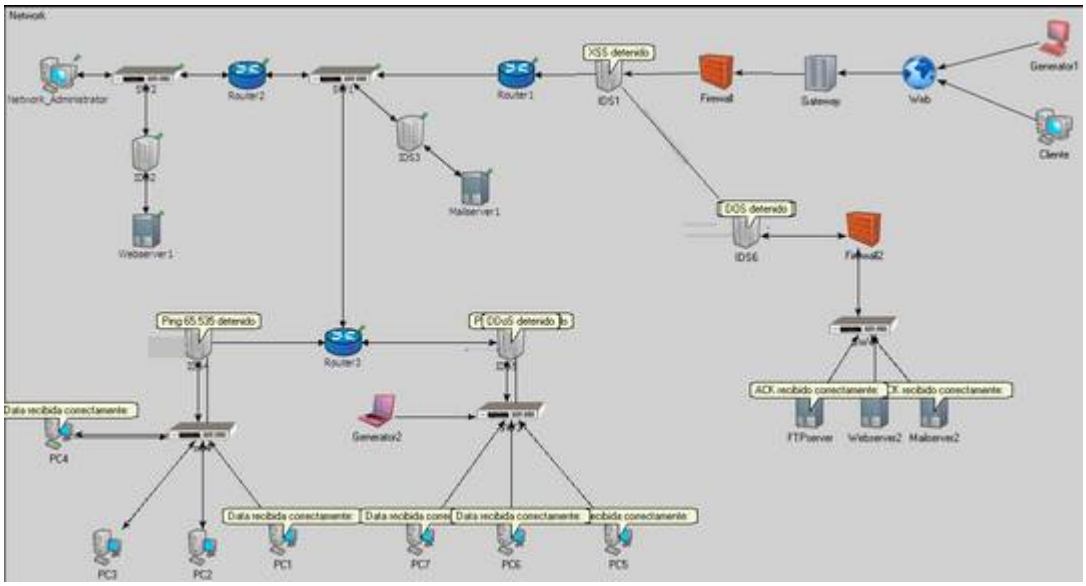


Figura 6.19: Detección de los ataques generados a través de los IDS en la simulación.

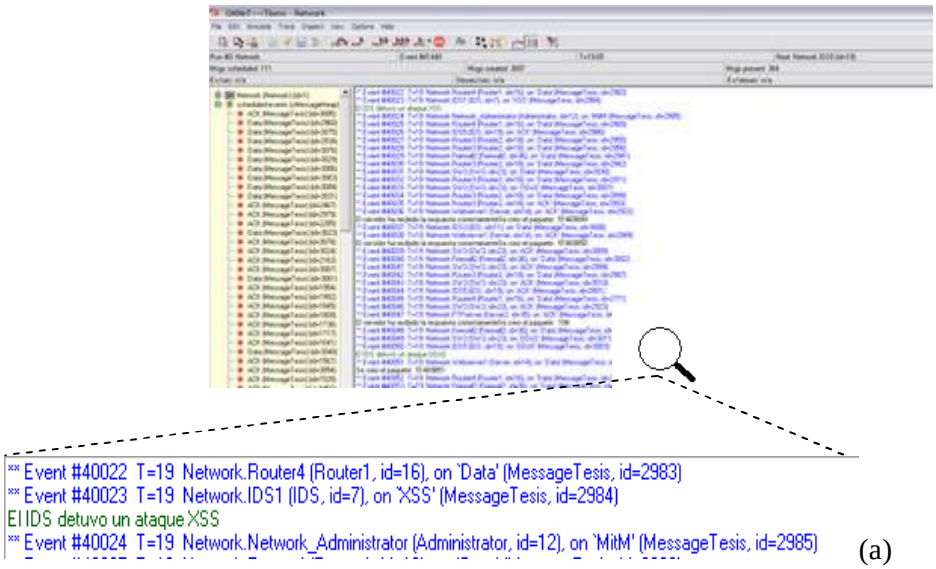
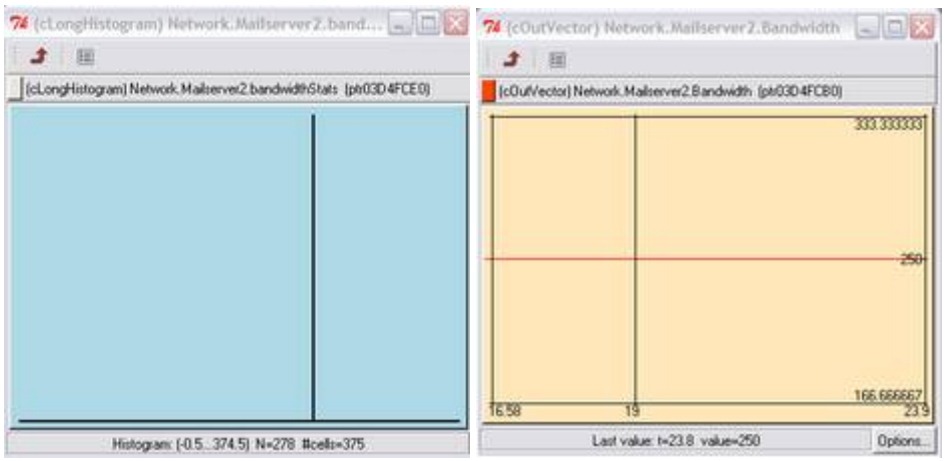
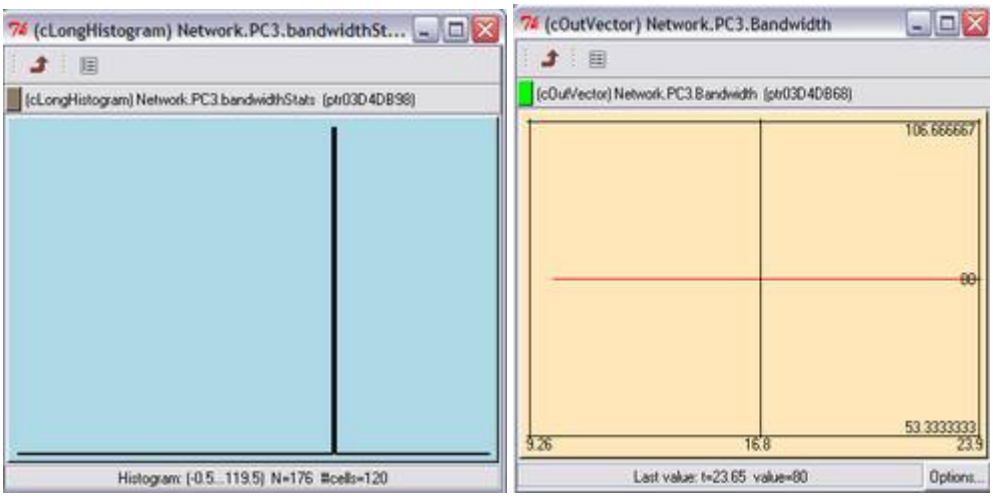


Figura 6.20: Registro de los eventos ocurridos durante la simulación. (a) Detección del ataque XSS. (b) Detección del ataque DDoS. (c) Generación de ataques XSS por el Generador de ataques 2 y DoS por el Generador de ataques 1.

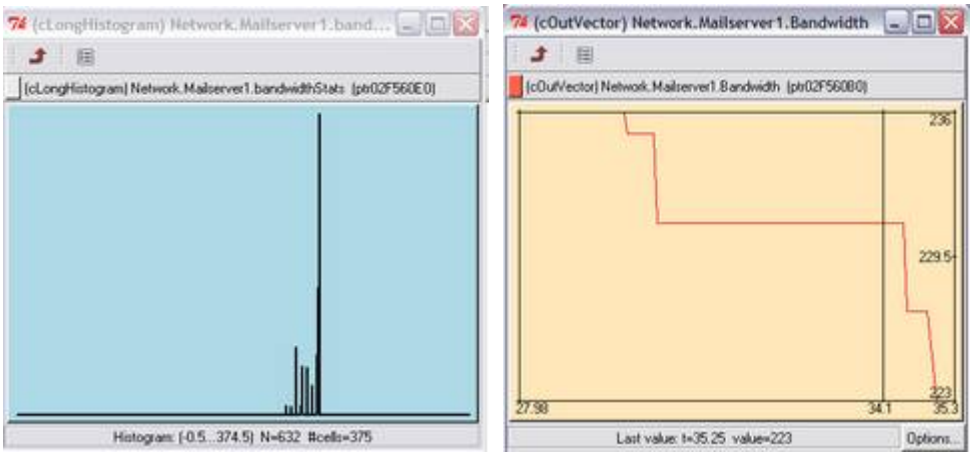
Al momento de ocurrir la creación de los ataques y posteriormente su detección, en la ventana *TKENV* se registran dichos eventos mostrando el o los paquetes detectados y el tiempo (véase la Figura 6.20). Dicha tabla permite conocer el tiempo en que ocurrieron los eventos, el origen y destino puesto que cada paquete cuenta con un número de identificación.



(a)



(b)



(c)

Figura 6.21: Comportamiento del BW para los nodos MailServer2 (a), PC3 (b) y MailServer1 (c).

En el bloque anterior se muestran las gráficas del comportamiento del BW de algunos de los nodos en la red (véase la Figura 6.21). Para estos resultados se emplearon tres elementos: MailServer2, Mail Server 1 y PC3.

Como se muestra en la Figura 6.21 en las imágenes (a) y (b) el BW de los elementos seleccionados no se afecta puesto que los IDS detectaron de manera oportuna los ataques que transitaban por la red. Por otra parte en la figura (c) el BW del MailServer1 se ve afectado ya que uno de los ataques pudo no ser detectado (Indicado en la Tabla 6.5) y no ser detectado por el IDS.

Esto fue programado intencionalmente en la ventana de *OMNETini* con el objetivo de mostrar resultados con los *Falsos negativos y los Falsos positivos.* Más adelante en la Figura 6.22 se muestra a otra víctima que es la PC7 y cuyo comportamiento del BW se afecta por los ataques. Cabe recordar que un falso negativo es la **No** detección de un intruso por el IDS y por lo tanto este puede afectar algún elemento o sistema en la red (véase la Figura 6.21 (c)). Mientras que un falso positivo es la detección de paquetes o archivos como posibles ataques sin que lo sean.

A continuación se muestran los valores estadísticos sobre el comportamiento del mismo recurso que ha sido objeto de análisis en este trabajo, el BW (véase la Figura 6.22).

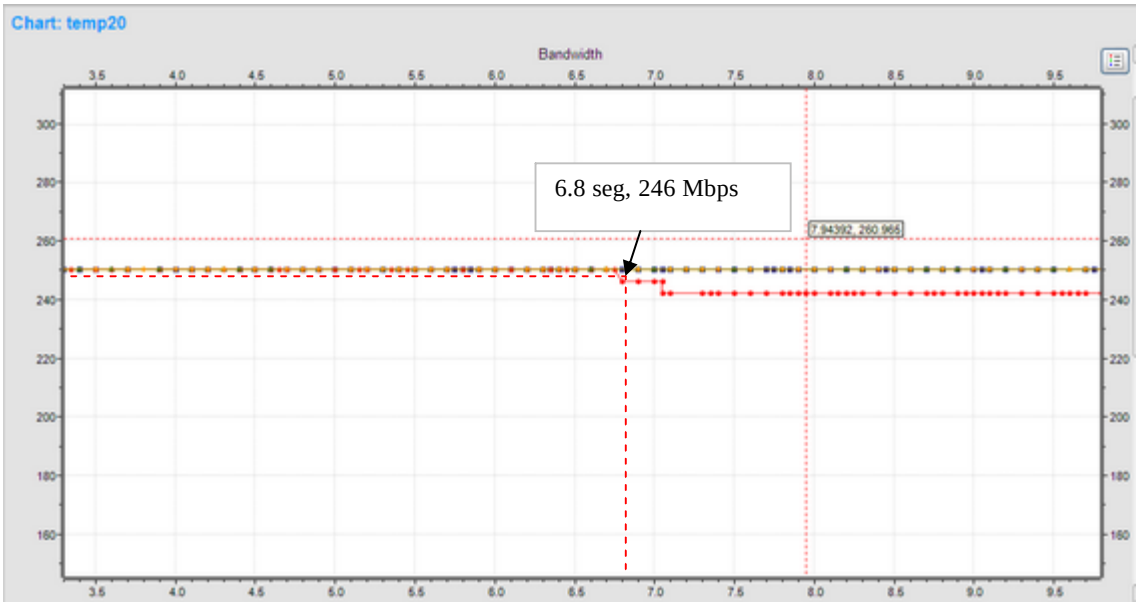


Figura 6.22: Comportamiento del BW de los servidores en la red. Los elementos seleccionados son: MailServer1 (Rojo), MailServer2 (verde), WebServer1 (Azul) y WebServer2 (amarillo).

Como se observa en la Figura 6.22, el WebServer1 fue el único servidor afectado en la red siendo a 6.8 segundos afectado su Bw decrementando a 246 Mbps de 250 Mbps establecidos inicialmente.

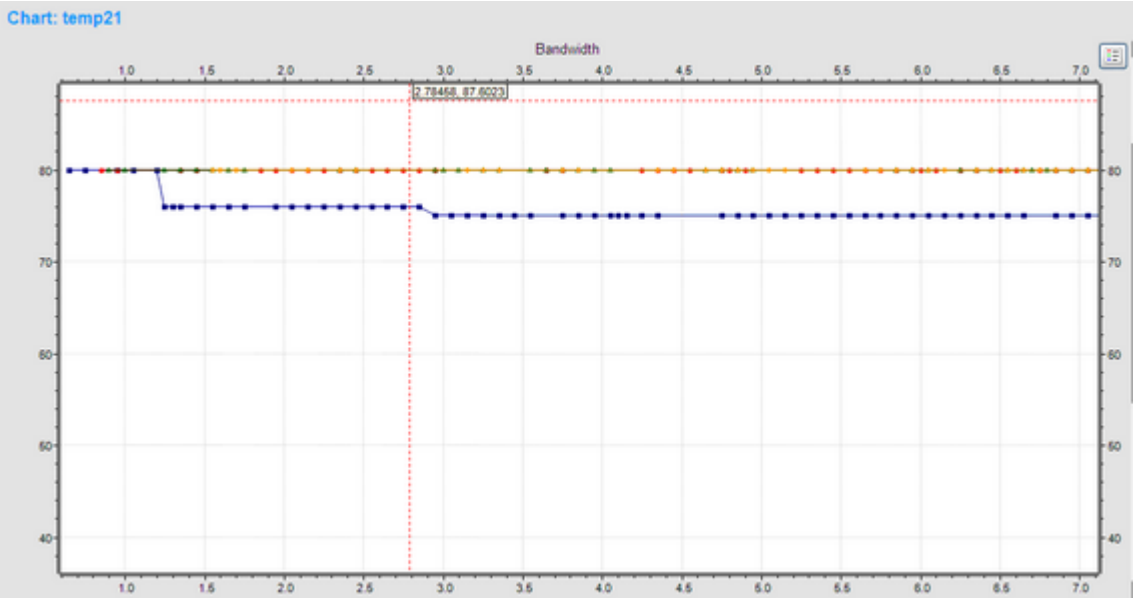


Figura 6.23: Comportamiento del BW de las PCs. La gráfica azul se enfoca en la PC7.

En la Figura 6.23 se muestra el BW en este caso enfocado el las PCs, tal como se observa en la gráfica, las PCs no se afectan en su BW excepto la PC7, que en el tiempo 1.33 segundos de la simulación el BW disminuyó a 73.7 Mbps.

Se muestran los valores estadísticos de los ataques que provocaron el inicio de la afectación en el BW de los dos elementos mencionados (Véase la figura 6.24). Posteriormente en la Tabla 6.5 se indican los siguientes valores registrados.

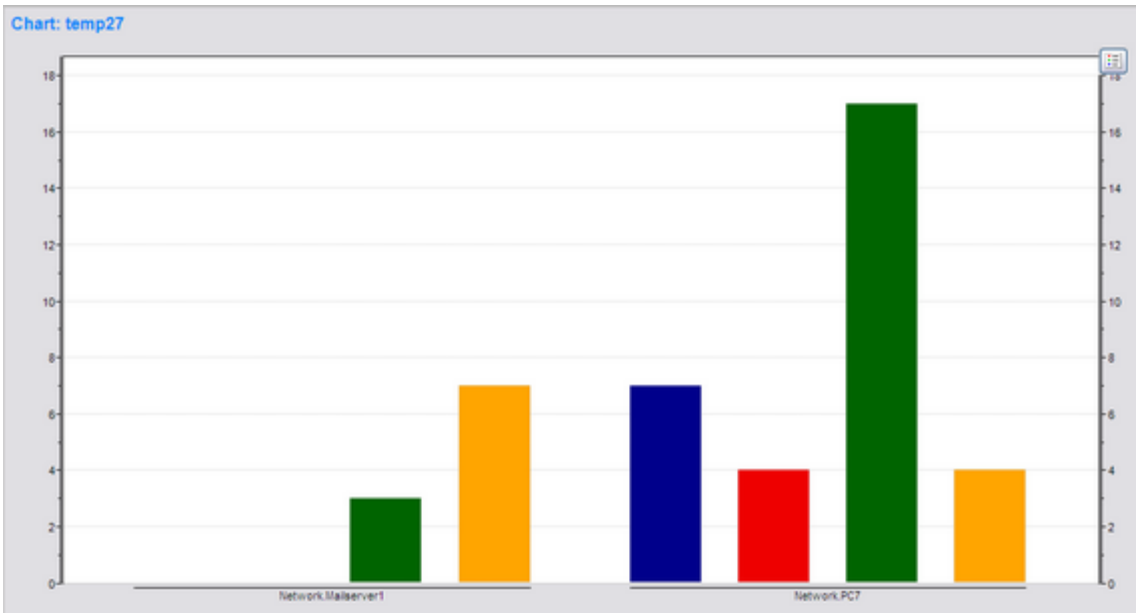


Figura 6.24: Valores estadísticos de los ataques recibidos en los elementos MailServer1 y PC7.

Tabla 6.5. Ataques registrados por las víctimas durante la simulación con IDS activados.

Elementos de la Red	Ataques Ping de la muerte	Ataque DoS	Ataque DDoS	Ataque Xss	Variación del Bw
MailServer1	3	0	7	0	A los 6.8 segundos decrementó a 246 Mbps.
PC7	17	4	7	4	A los 1.3 segundos decrementó a 73.7 Mbps.

Una vez registrados los ataques y los elementos de la red afectados, se muestran la detección y registro de los ataques por parte de los sistemas para detección de intrusos (Véase la Figura 6.25)

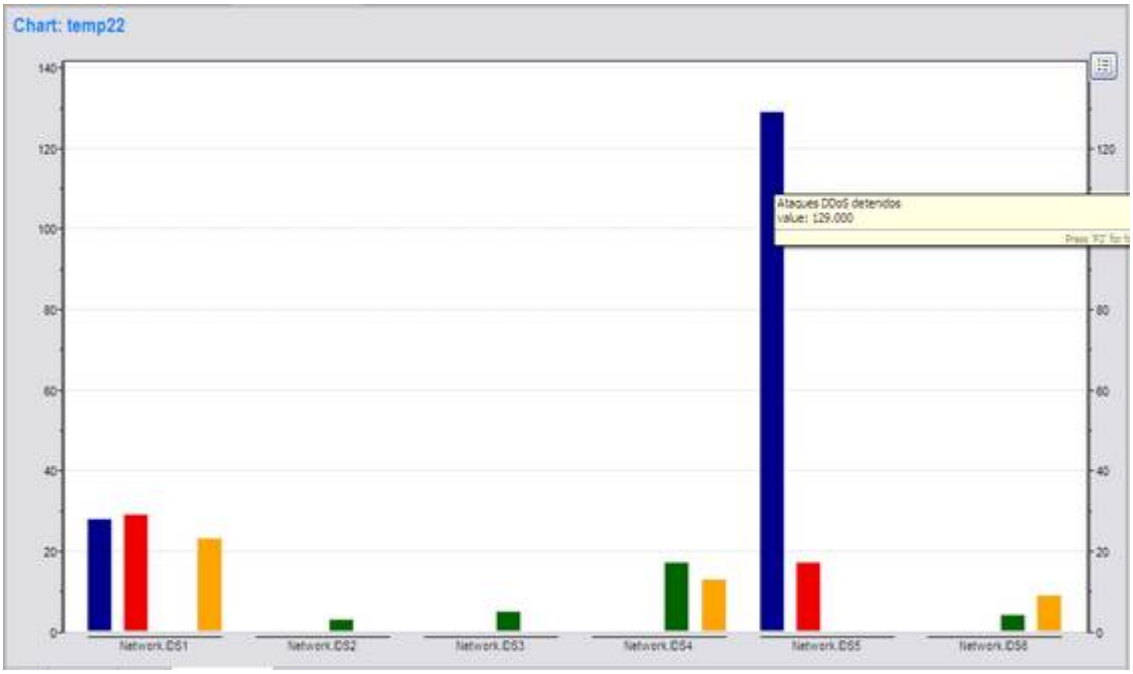


Figura 6.25: Detección de los ataques por parte de los IDS.

Tabla 6.6. Ataques detectados y registrados por los IDS.

IDS	Ataques Ping de la muerte	Ataque DoS	Ataque DDoS	Ataque Xss	Total
IDS1	0	29 IP de procedencia 159.16.139.78.	28 IP de procedencia 159.16.139.78.	23 IP de procedencia 159.16.139.78.	80
IDS2	3 IP de procedencia 159.16.139.78	0	5 IP de procedencia 10.24.148.12	0	8
IDS3	5 IP de procedencia 159.16.139.78	0	0	0	5
IDS4	17 IP de procedencia 159.16.139.78.	0	0	13 IP de procedencia 10.24.148.12	30

	Provocó 3. 10.24.148.12 Provocó 14.			Provocó 9. IP de procedencia 159.16.139.78. Provocó 4.	
IDS5	0	17 IP de procedencia 10.24.148.12	124 IP de procedencia 10.24.148.12	0	141
IDS6	4 IP de procedencia 159.16.139.78	0	0	9 IP de procedencia 159.16.139.78	13
Total de ataques detectados					**277**

En la Tabla 6.6 se muestran también las direcciones IPs de procedencia, dichas direcciones se refieren a los Generadores de ataques, en el que *159.16.139.78* es el Generador de ataques 1 y *10.24.148.12* es el Generador de ataques 2. El total de ataques detectados por el IDS diseñado fue de 272.

Las direcciones IP registradas en la Tabla 6.6 fueron obtenidas a través de la herramienta *TKENV* en el que se muestra el ataque generado por alguno de los generadores, el cual contiene un número de identificación, y que al llegar al IDS el ataque correspondiente, este se indica en la misma ventana de eventos, a través del mismo número de identificación y en base al periodo de duración de la simulación, que para este caso fue de 19.8 segundos.

Del mismo modo se realizó la comparación del desempeño del Firewall ante los ataques MiTM. En la Figura 6.26 se muestran estadísticas de este ataque a través de los Firewall sobre la red.

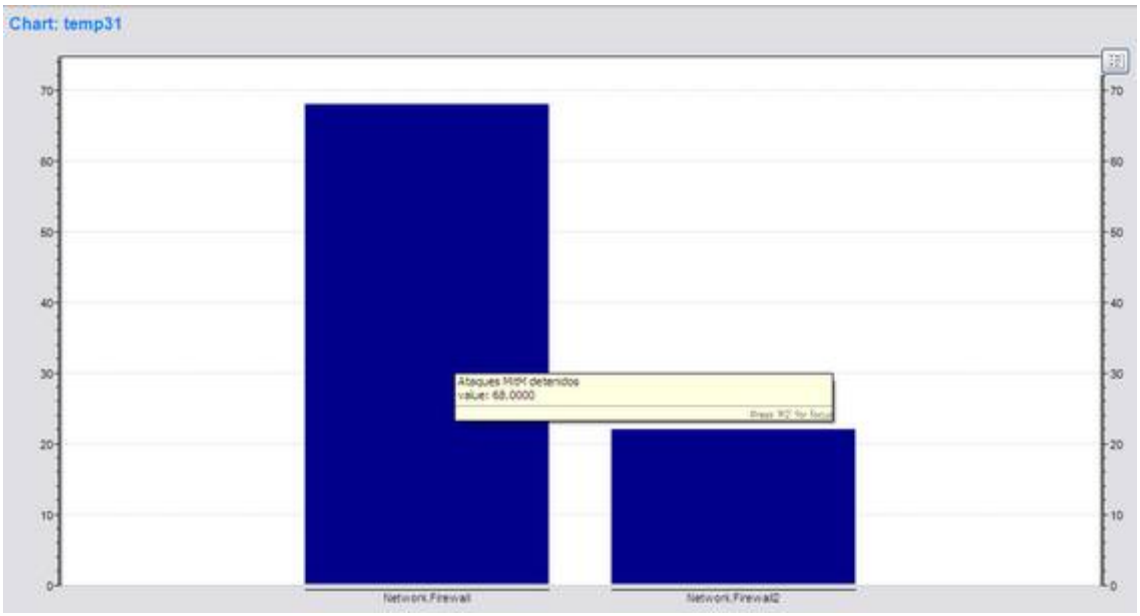


Figura 6.26: Detección de los ataques MiTM por parte de los Firewall.

Los ataques que registraron los firewall fueron los siguientes.

Tabla 6.7. Ataque MiTM detectados por los Firewall.

Firewall	Ataques MiTM
Firewall 1	68 IP de Procedencia 159.16.139.78
Firewall 2	24 IP de Procedencia 10.24.148.12

6.7.1 Falsos Negativos y Falsos Positivos

Los resultados que se obtuvieron en la simulación muestran el desempeño de los IDS ubicados en diferentes puntos de la red. Con el fin de simular el ambiente de una red se realizó la activación de cada uno de estos sistemas para que se detectaran ciertos ataques ocurriendo así los falsos negativos y positivos para así medir la eficiencia del IDS diseñado en base a las amenazas detectadas y no detectadas (véase la Figura 6.27).

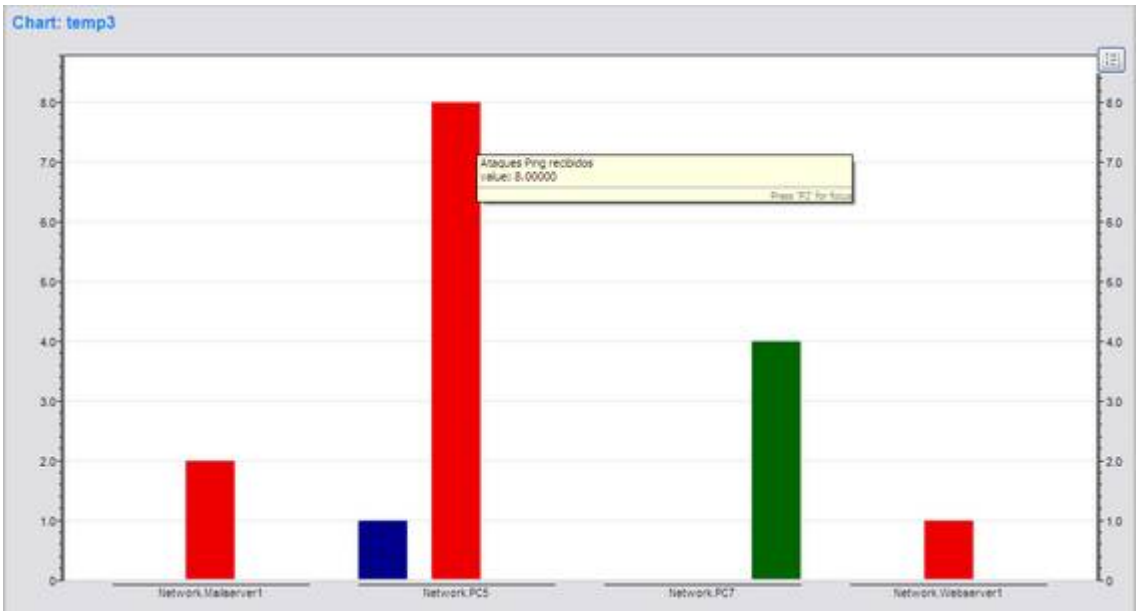


Figura 6.27: Ataques no detectados por los sistemas de detección de intrusos. Elementos afectados MailServer1, PC5, PC7 WebServer1.

En la Figura 6.27 se muestran los ataques que no fueron detectados por los IDS afectando el sistema de los nodos MailServer1 y PC7. Los ataques que afectaron a estos sistemas se encuentran registrados en la Tabla 6.5. A continuación en la Tabla 6.8 se presenta el registro de los falsos negativos y en la Tabla 6.9 de los falsos positivos para cada uno de los IDS ubicados en la red (véase la Figura 6.28). La Tabla 6.8 muestra la desactivación de los IDS para cada ataque.

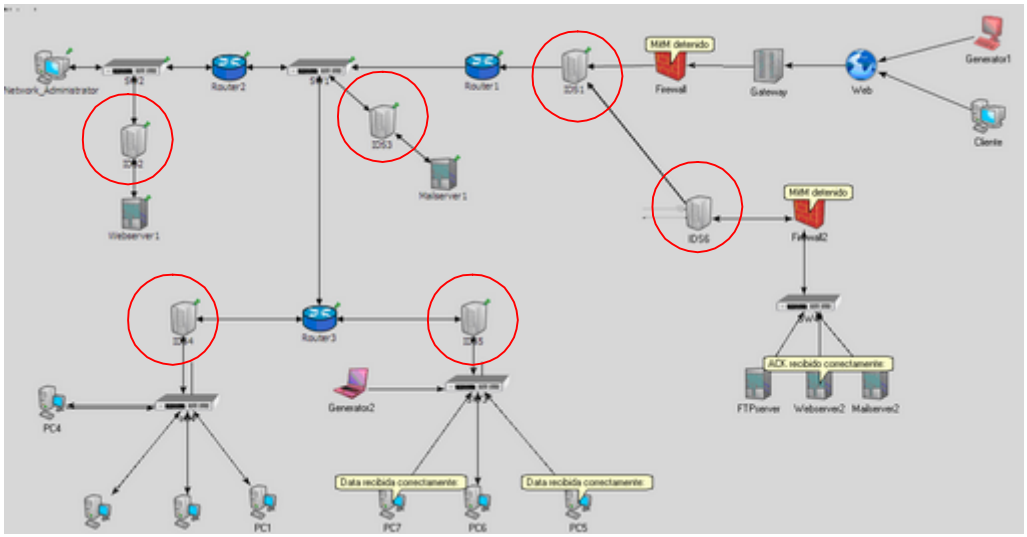


Figura 6.28: Ubicación de los IDS en la red diseñada. Su colocación está marcada con círculo rojo.

Tabla 6.8. Registro de los falsos negativos.

IDS	Falsos Negativo	Cantidad
IDS1	PoD	2
IDS2	XSS	2
IDS3	DDoS	7
IDS4	DoS	4
IDS5	PoD	8
IDS6	DDoS	1
IDS6	MiTM	24
Total de Falsos negativos		**48**

Tabla 6.9. Registro de los falsos positivos.

IDS	Falsos Positivo	Cantidad
IDS1	Data→PoD	1
IDS2	Data→XSS	1
IDS3	ACK→DDoS	5
IDS4	Data→DoS	1
IDS5	ACK→	6
IDS6	ACK→DoS	2
IDS6	Data→MiTM	4
Total de Falsos positivos		**20**

En la Tabla 6.8 se muestran los valores estadísticos en relación a los falsos negativos o amenazas que no fueron detectadas por los IDS indicados, dando un total de 48 falsos negativos de los cuales hay 24 ataques MiTM que posteriormente fueron detectados por el Firewall de la DMZ, los valores de detección de este ataque se muestran en la Tabla 6.7.

Mientras que en la Tabla 6.9 se muestra el registro de los falsos positivos en cada uno de los IDS incluidos los cuales fueron 20 registrados; la esta detección se ha dado en el momento en que el IDS detecta un ataque y el paquete que le prosigue es detectado como una amenaza por cuestión de seguridad con el objetivo de evitar un desarrollo del ataque detectado, esto de acuerdo al diseño establecido en el IDS.

En el bloque con título de falsos positivos de la misma tabla se indica primero el mensaje o paquete detectado como ataque y a continuación el ataque provocó el falso positivo. Estos valores registrados en la tabla se obtuvieron por medio de la herramienta *TKENV*.

El porcentaje de desempeño del IDS diseñado se midió en función de los ataques detectados y de los falsos negativos y positivos registrados durante la simulación, tomando como muestra los valores de las Tablas 6.6, 6.8 y 6.9 en el que el 100% de eficiencia de cada IDS se basa en los ataques detectados y la deficiencia en los falsos negativos y positivos (véase la Tabla 6.10).

Tabla 6.10. Porcentaje de eficiencia del IDS diseñado.

IDS	**% Eficiencia en la detección de intrusos**
IDS1	**98%**
IDS2	**80%**
IDS3	**88%**
IDS4	**88%**
IDS5	**99%**
IDS6	**95%**
Eficiencia total de los IDS en la Red	**95%**

En la Tabla 6.10 se presentan los porcentajes de efectividad para la detección de intrusos de cada IDS, y que en conjunto representan el nivel de desempeño en la detección de intrusos para el sistema de seguridad diseñado siendo del 95% de efectivo ante la detección de amenazas. Cabe mencionar que este nivel de desempeño se obtuvo en razón de la desactivación de ciertos ataques en los IDS ya que de llevarse acabo la activación para detectar todos los ataques generados en la red el desempeño será del 100%.

En conclusión a este capítulo, los ataques empleados para realizar las pruebas se consideraron debido a la manera en cómo se afecta a la víctima. El recurso empleado como análisis para estas pruebas fue el BW de los servidores y PCs sobre la red, por otra parte la función que tiene el usuario del simulador al analizar los ataques es la de un Administrador de Red (*Network Administrator*) puesto que tiene la capacidad de visualizar los eventos ocurridos en la red durante la ejecución de la simulación.

6.7 Discusión

En este capítulo se han presentado las pruebas y los resultados de la simulación en base a los parámetros establecidos tales como el retardo de transmisión en los enlaces de los nodos, el tiempo de generación del tráfico y de los ataques y el ancho de banda para cada elemento en la red. Se realizó el análisis del tráfico compuesto por ataques y paquetes o datos para comparar el efecto sobre el ancho de banda de los elementos de la red, el cual fue el objeto de análisis para posteriormente medir el desempeño del IDS diseñado. Dichos valores se encuentran registrados en las tablas de los valores obtenidos en las pruebas realizadas en la simulación.

El IDS diseñado para esta simulación tiene un desempeño del 93% en el que la efectividad del sistema se obtuvo comparando los valores de los ataques registrados y los falsos negativos. Por otra parte los Firewall establecidos en la red realizaron la detección del ataque MiTM en un 100% pero no de las otras amenazas detectadas por los respectivos IDS.