INGENIERÍA Y DESARROLLO

ARTÍCULO DE INVESTIGACIÓN / RESEARCH ARTICLE
http://dx.doi.org/10.14482/inde.32.1.5196

Validación de la caracterización estadística del tráfico de red de un servidor web de un campus universitario como mecanismo de un sistema de detección de intrusos

Validation of the statistical characterization of the web server's network traffic in a university campus as a mechanism of an intrusion detection system

Antonio Hernández Jaimes*
Lina Prada Angarita**
Universidad del Norte (Colombia)

* Ingeniero de Sistemas, Especialista en Telecomunicaciones, Magíster en Telemática y Telecomunicaciones en la Universidad del Norte; Especialista en Seguridad Informática en la Universidad Pontificia Bolivariana; EC Council Disaster Recovery Professional, GIAC Security Essentials (GSEC) Professional; Certificate of Cloud Security Knowledge (CCSK), Administrador de Seguridad Informática, Universidad del Norte. *ahernand@uninorte.edu.co*

** Ingeniera Industrial, Candidata a Magister en Ingeniería Industrial de la Universidad del Norte; Profesora tiempo completo, Departamento ~~de Ingeni~~ería Industrial, Universidad del Norte. *pradal@uninorte.edu.co*

Correspondencia: Antonio Hernández Jaimes, Km. 5 Vía Puerto Colombia. Dirección Tecnología Informática y de Comunicaciones, Primer Piso, Bloque B, Tel: 57+5+3509772.

Volumen 32, n.º 1
Enero-junio, 2014
ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Resumen

El presente artículo muestra el resultado del análisis estadístico del tráfico de red (expresado en bits por segundo) desde y hacia el servidor web de un campus universitario. El análisis estadístico permite conocer las tendencias del tráfico por hora y establecer una línea base para un comportamiento normal. Se documentan, además, los resultados de las pruebas de bondad y ajuste, y los análisis de varianza, los cuales proporcionan elementos que enriquecen la definición de la línea base. Finalmente, los hallazgos son examinados para determinar su utilidad como mecanismo de detección de intrusos o de situaciones que sugieran anomalías o comportamientos atípicos en el tráfico.

Palabras clave: IDS, seguridad informática, tráfico de red.

Abstract

This paper presents the results of statistical analysis of network traffic (in bits per second) from and to one university web server. Statistical analysis allows to know the hourly traffic trends and to establish a baseline for normal behavior. It documents, in addition, statistical goodness-fit tests results and analysis of variance, which provide elements that enhance the definition of the baseline. Finally, the outcomes are analyzed to determine its usefulness as intrusion detection mechanism or situations or behaviors that could suggest anomalies or atypical traffic.

Keywords: IDS, information security, network traffic.

Fecha de recepción: 5 de agosto de 2013
Fecha de aceptación: 2 de diciembre de 2013

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

1. INTRODUCCIÓN

El tráfico de red de un servidor web es motivo de estudio y análisis en la mayoría de las organizaciones. También es motivo de preocupación puesto que gran cantidad de amenazas informáticas son explotadas a través de protocolos y puertos permitidos como HTTP (protocolo de transferencia de hipertexto) o HTTPS (protocolo de transferencia de hipertexto seguro). Además, se estudia para realizar predicciones de crecimiento de ancho de banda, *caching* y contenido, permitiendo así diseñar nuevas soluciones de administración [1], [2].

Conocer lo que se transmite por la red y poderlo caracterizar es imperativo para los administradores o ingenieros de seguridad si se quiere detectar anomalías en el tráfico. En la medida en que se sepa "lo que acontece" en la red, se podrán detectar más rápidamente posibles ataques y, por ende, contener y minimizar su efecto malicioso. La principal finalidad de un sistema de detección de intrusos (IDS) es monitorear la actividad en un servidor o en una red, de tal manera que se puedan obtener pistas y alertas de posibles ataques o intentos de violación a la seguridad. En otras palabras, un IDS identifica actividad "no deseada", genera alarmas y utiliza mecanismos de detección de estos eventos no deseados, los cuales están basados normalmente en patrones de comportamiento, firmas de código o análisis de protocolos. Sin embargo, los mecanismos no son perfectos y pueden presentarse comportamientos fallidos del sistema, los cuales se clasifican en:

- Falsos positivos: el IDS genera una alarma ante un evento que en realidad corresponde con un comportamiento normal.

- Falsos negativos: el IDS no genera alarma ante un evento malicioso, es decir, falla en la detección.

Trabajos como los expuestos en [3], [4] y más recientemente en [5], construyen una línea base (*baseline*) a partir de la cual puede describirse un comportamiento esperado del tráfico de red en condiciones normales, lo cual es útil como mecanismo para la detección de situaciones anómalas o ataques.

Hoy día las investigaciones se centran en diseñar y construir IDS cada vez más confiables y en fortalecer su valor como activos de la infraestructura

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

de seguridad de una compañía [6]. IDS más confiables significa tener menor número de falsos positivos y falsos negativos. El uso de la estadística y de la teoría de cadenas de Markov resulta útil en el diseño de nuevos y más confiables mecanismos en los IDS [7]. También pueden combinarse estrategias de detección para lograr esquemas híbridos y adaptativos [8]. En últimas, lo que se persigue es que los modelos sean fáciles de implementar, rápidos en su análisis de reglas y que sean confiables en las alarmas que generan.

El tráfico es una variable que difiere en su comportamiento dependiendo del servicio (contenido web, correo electrónico, sistemas de monitoreo y alarma, etc.). Los análisis documentados en artículos científicos normalmente son generales y no están enmarcados dentro de un contexto. Lo anterior hace que el aporte más importante del presente ejercicio sea el análisis estadístico que se realiza al tráfico que caracteriza a un servidor web de un campus universitario, es decir, en un contexto puntual de este servicio. Este análisis estadístico es validado como mecanismo de detección de intrusos.

2. METODOLOGÍA

La metodología utilizada en el desarrollo del presente análisis se describe a continuación:

Recolección de los datos: los datos a analizar se recolectaron utilizando el monitor de desempeño del sistema operativo Windows del servidor web principal de un campus universitario. La herramienta midió los valores de tráfico de entrada y de salida (utilización de la interfaz de red del servidor web) cada cinco minutos en unidades de bits por segundo. Los datos fueron recolectados durante tres meses y una semana, lapso de tiempo que abarcó tres momentos importantes: el proceso de matrícula, el inicio del semestre académico y el reporte de calificaciones de los primeros y segundos parciales, procesos durante los cuales son altamente utilizados los servicios alojados en el sitio web del campus universitario. El intervalo de monitoreo usado fue de cinco minutos, porque es el más utilizado en las herramientas de monitoreo [9] [10]. Para el caso de un servidor con sistema operativo *nix, los datos pueden recopilarse con una la utilidad *nstat* o cualquier utilidad para medir utilización de la interfaz de red.

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Consolidación de los datos: los datos recolectados fueron agrupados por hora. Para efectos del análisis estadístico, y teniendo en cuenta que se trata de estudiar jornadas típicas, se eliminaron los datos correspondientes a días domingos y festivos.

Análisis de los datos: los datos recolectados y agrupados por hora fueron consolidados en un libro de Microsoft Excel. Con esta herramienta se generaron los histogramas del tráfico de entrada y de salida (ver figuras 1 y 2) y se calcularon los valores que caracterizan al tráfico: medias, desviaciones estándar, máximos, mínimos. Con la herramienta Xlstat [11] se realizaron las siguientes pruebas de bondad y ajuste:

- Pruebas de normalidad de Shapiro-Wilk, Anderson-Darling, Kolmogorov-Smirnov, Chi-cuadrado, Lilliefors y Jarque-Bera (tráfico de entrada y tráfico de salida).

- Pruebas de bondad y ajuste de Kolmogorov-Smirnov y de Chi-cuadrado para distribuciones Fisher, Chi-cuadrado y Erlang.

Análisis de varianza: utilizando el paquete de *software* Statgraphics Centurion se realizaron análisis de varianza (Anova) para los datos correspondientes al tráfico por hora.

Validación del modelo: la utilidad del modelo como mecanismo de un sistema de detección de intrusos fue corroborada con la simulación de un ataque de denegación de servicio, el cual ocupa toda la capacidad del enlace de manera constante durante un período de tiempo.

3. RESULTADOS Y DISCUSIÓN

En el análisis estadístico realizado fueron utilizadas las siguientes herramientas: la descripción de los datos para lograr una representación básica; las pruebas de bondad y ajuste, para determinar si el tráfico sigue una distribución de probabilidad conocida; y finalmente, el análisis de varianza, para describir la heterogeneidad de los datos.

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Análisis descriptivo

A continuación se exponen los resultados del análisis descriptivo de los datos consolidados. La tabla 1 muestra los valores (en bps) para el tráfico de entrada:

Tabla 1. Tráfico de entrada

Variable	Entrada
Observaciones	10.835,00
Mínimo	1,00
Máximo	999.917,00
Media	448.110,14
Desviación típica	307.700,22

La figura 1 muestra el histograma del tráfico de entrada:

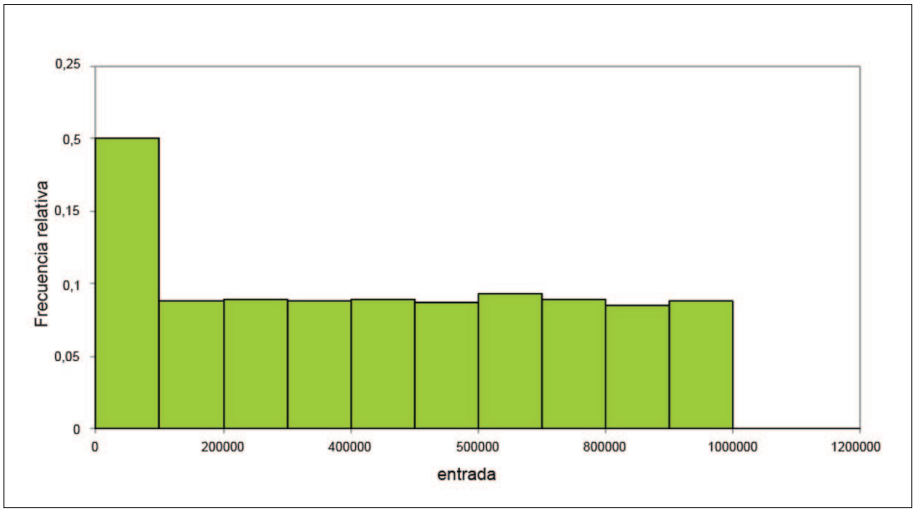

Figura 1. Histograma de tráfico de entrada.

La tabla 2 contiene los valores en bits por segundo (bps) para el tráfico de salida:

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Tabla 2. Tráfico de salida

Variable	Salida
Observaciones	10.835,00
Mínimo	0,00
Máximo	999.617,00
Media	445.431,70
Desviación típica	305.351,92

La figura 2 ilustra el histograma del tráfico de salida:

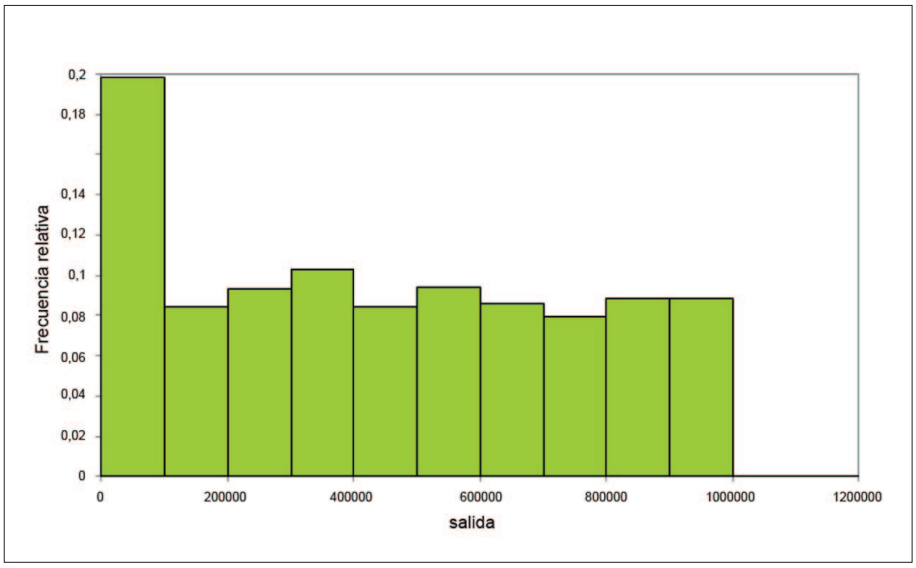

Figura 2. Histograma tráfico de salida.

Pruebas de bondad y ajuste

Se realizaron pruebas de bondad y ajuste para determinar la normalidad de los datos correspondientes al tráfico de entrada y de salida por hora. Como hipótesis nula H0 se planteó que la variable de la cual se extrajo la muestra sigue una distribución normal; y como hipótesis alterna Ha, que la variable de la cual se extrajo la muestra no sigue una distribución normal. Se utilizó un nivel de significación (a) de 0,05. En todos los casos el p-valor

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

computado resultó menor que el nivel de significación alfa = 0,05, por lo que se rechazó la hipótesis nula H0, es decir, no existe evidencia estadísticamente significativa de la normalidad. Los resultados están consignados en la tabla 3:

Tabla 3. Pruebas de normalidad para el tráfico de entrada y de salida

		Tráfico de entrada		Tráfico de salida	
Prueba	**E**	**Valor**	**Resultado**	**Valor**	**Resultado**
Kolmogorov-Smirnov	D	0,081	Rechazar	0,075	Rechazar
Chi-Cuadrado	X2	5482,54	Rechazar	5369,99	Rechazar
Shapiro-Wilk	W	0,937	Rechazar	0,940	Rechazar
Anderson-Darling	A^2	182,49	Rechazar	171,86	Rechazar
Lilliefors	D	0,081	Rechazar	0,075	Rechazar
Jarque-Bera	JB	768,67	Rechazar	747,32	Rechazar

Además, se realizaron pruebas para determinar la posible normalidad de los datos del tráfico aislando horas específicas. Los valores de los estadígrafos obtenidos no arrojaron evidencia de normalidad. La tabla 4 muestra estos resultados:

Tabla 4. Pruebas de normalidad para el tráfico de entrada y de salida en horas aisladas

			Tráfico de entrada		Tráfico de salida	
Prueba	**Hora**	**E**	**Valor**	**Resultado**	**Valor**	**Resultado**
Kolmogorov-Smirnov	00:00	D	0,096	Rechazar	0,092	Rechazar
Chi-cuadrado	00:00	X^2	277,554	Rechazar	260,959	Rechazar
Kolmogorov-Smirnov	10:00	D	0,078	Rechazar	0,080	Rechazar
Chi-cuadrado	10:00	X^2	164.472	Rechazar	225,835	Rechazar
Kolmogorov-Smirnov	16:00	D	0,102	Rechazar	0,071	Rechazar
Chi-cuadrado	16:00	X^2	237,337	Rechazar	224,795	Rechazar

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Se realizaron otras pruebas de bondad y ajuste para determinar si los datos siguen distribuciones de Fisher, Chi-cuadrado o Erlang. Sin embargo, como se nota en la tabla 5, no existe evidencia estadística para afirmar que los datos siguen alguna de estas distribuciones de probabilidad.

Tabla 5. Otras pruebas de bondad y ajuste para el tráfico de entrada y de salida

		Tráfico de entrada		Tráfico de salida	
Prueba	**E**	**Valor**	**Resultado**	**Valor**	**Resultado**
Kolmogorov-Smirnov para Fisher	D	1,000	Rechazar	0,999	Rechazar
Kolmogorov-Smirnov para Chi-cuadrado	D	0,505	Rechazar	0,514	Rechazar
Kolmogorov-Smirnov para Erlang	D	0,388	Rechazar	0,390	Rechazar

El tráfico como un proceso estocástico

Papoulis [12] define un proceso estocástico como la colección de todas las posibles realizaciones o resultados de las observaciones de un experimento o evento que ocurre n veces. Para el caso del servidor web, se consideró el tráfico de una hora determinada como una variable aleatoria, como se muestra en la figura 3:

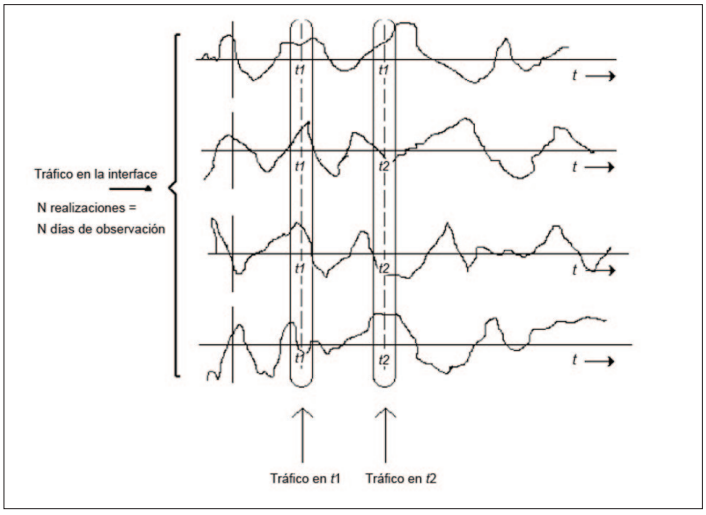

Figura 3. El tráfico como variable aleatoria.

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Al graficar los valores de tráfico por hora como variables aleatorias y realizaciones diarias se observó cierta estabilidad en las medias, como lo muestra la figura 4:

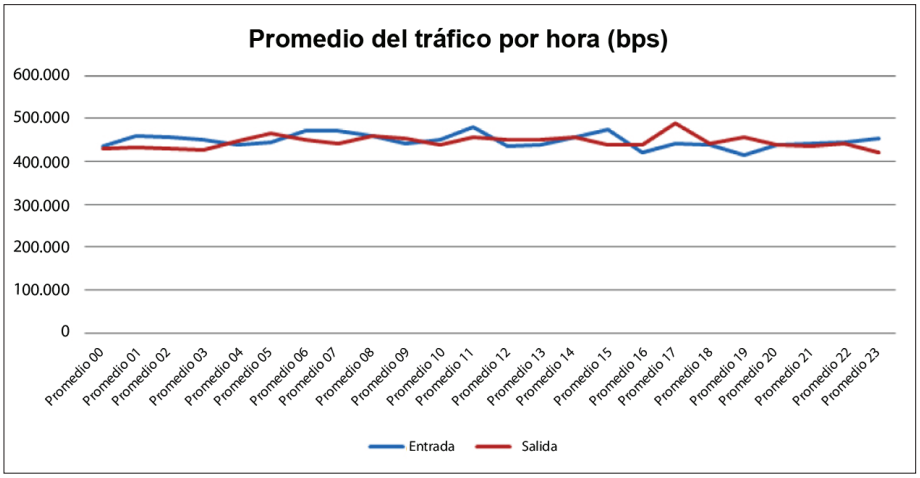

Figura 4. Promedio del tráfico por hora.

Para los valores de las desviaciones estándar se tiene un hallazgo similar:

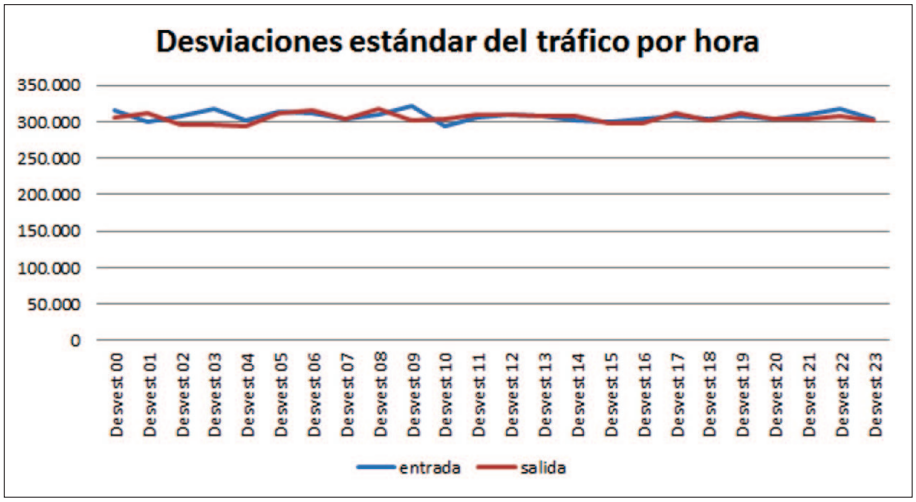

Figura 5. Desviaciones estándar del tráfico por hora.

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Sin embargo, fue a través de un análisis de varianza (Anova) que se pudo evidenciar la estabilidad de estos parámetros.

Análisis de varianza

Para realizar este análisis se consideró que cada hora del día es una población. Se pretende probar qué tan diferentes estadísticamente son los valores de media y desviación estándar del tráfico de entrada y salida para cada momento del día. La tabla 6 muestra el Anova utilizado para descomponer la varianza de los valores del tráfico de entrada en dos componentes: un componente "entre grupos" y un componente "dentro de grupos". Cada grupo es una hora del día (de 0 a 23). La razón-F, que en este caso es igual a 1,22985, es el cociente entre el estimado entre grupos y el estimado dentro de grupos. Puesto que el valor-P de la razón-F es mayor o igual que 0,05, no existe una diferencia estadísticamente significativa entre la media entre un nivel de hora y otro, con un nivel del 95,0% de confianza. Así mismo, el estadístico de Levene's evalúa la hipótesis de que la desviación estándar de entrada dentro de cada uno de los 24 niveles de hora es la misma. Puesto que el valor-P es mayor o igual que 0,05, no existe una diferencia estadísticamente significativa entre las desviaciones estándar, con un nivel del 95,0% de confianza.

Tabla 6. Anova para el tráfico de entrada y de salida

		Tráfico de entrada		Tráfico de salida	
Fuente - Prueba	**GL**	**Razón-F**	**Valor-P**	**Razón-F**	**Valor-P**
Entre grupos (entre horas)	23	1,22985	0,2055	1,06	0,3867
Levene's			0,53267		0,36076

Es decir que, tanto para el tráfico de entrada como para el de salida, se puede considerar que las medias y las desviaciones estándar de los valores entre las diferentes horas de observación no varían significativamente en el tiempo. Esta es una condición necesaria, pero no suficiente para que el tráfico sea considerado un proceso estacionario en el tiempo [12].

Validación del modelo

El hallazgo más importante del análisis realizado es que las medias del tráfico por hora no varían, es decir, que pueden considerarse constantes.

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

Este comportamiento puede tomarse como línea base y detectar situaciones o eventos anormales cuando las condiciones cambien. Para validar su utilidad como mecanismo de detección de intrusos, se consideró un ataque de denegación de servicio. Este tipo de ataque es el más difundido [13] y el que mayor impacto produce [14]. Recientemente se han propuesto mecanismos de mitigación del impacto de este tipo de ataques, pero dado que se ejecutan con tráfico y peticiones válidas, su detección y prevención resulta un verdadero reto [15], [16], [17].

En las pruebas realizadas se asumió que el ataque ocupaba al máximo el enlace de entrada durante un tiempo determinado. La tabla 7 muestra los resultados del Anova para el tráfico de entrada durante varios ataques de denegación de servicio con diferentes duraciones: 5 segundos, 10 segundos, 15 segundos y 60 segundos, respectivamente.

Tabla 7. Anova para el tráfico de entrada-simulación de ataque DoS de 5,10, 15 y 60 segundos

	5 s	**10 s**	**15 s**	**60 s**
Fuente-prueba	**Valor-P**	**Valor-P**	**Valor-P**	**Valor-P**
Entre grupos (Entre horas)	0,2030	0,1886	0,1865	0,0932

En todos los casos anteriores, puesto que el valor-P es mayor o igual que 0,05, no existe una diferencia estadísticamente significativa entre la media del tráfico de entrada entre un nivel de hora y otro, con un nivel del 95,0% de confianza. Lo cual significa que el ataque no puede ser detectado con el mecanismo planteado. Para el caso de un ataque con una duración de 90 segundos, los resultados fueron los siguientes:

Tabla 8. Anova para el tráfico de entrada-simulación de ataque DoS de 90 segundos

Fuente - Prueba	GL	Razón-F	Valor-P
Entre grupos (Entre horas)	23	1,57	***0,0402***

Es decir, que debido a que el valor-P de la prueba-F es menor que 0,05 (0,0402), existe una diferencia estadísticamente significativa entre la media de entrada entre un nivel de hora y otro, con un nivel del 95,0% de con-

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

fianza. Es decir, el IDS puede detectar un ataque de duración 90 segundos teniendo como mecanismo de detección el Anova realizado.

En la tabla 9 (generada por el Anova de Statgraphics) se identifican cuatro grupos homogéneos según la alineación de las X's en columnas. Se encontró que no existen diferencias estadísticamente significativas entre aquellos niveles que compartan una misma columna de X's. El método empleado para discriminar entre las medias es el procedimiento de diferencia mínima significativa (LSD) de Fisher. Con este método hay un riesgo del 5,0% al decir que cada par de medias es significativamente diferente, cuando la diferencia real es igual a 0. Nótese que las horas 11:00 y 19:00 son las que presentan las mayores diferencias (una sola X). Es decir, estadísticamente se pueden considerar las medias del tráfico de entrada de estas horas como diferentes a las de las demás horas. Este hallazgo es útil, puesto que el IDS puede ser configurado teniendo en cuenta este comportamiento, es decir, que existen algunas horas en las que el comportamiento del tráfico difiere de la media estable que se tiene preestablecida.

Tabla 9. Grupos homogéneos por hora del Anova.

Hora	*Casos*	*Media*	*Grupos homogéneos*		*Hora*	*Casos*	*Media*	*Grupos homogéneos*
19	***456***	***415654***	***X***		22	456	445240	XXX
16	456	419348	XX		10	455	449581	XXX
0	455	435114	XXX		3	445	450081	XXX
12	457	436654	XXX		23	455	454176	XXX
20	456	437393	XXX		2	455	454780	XXX
4	442	438207	XXX		14	456	456906	XX
18	456	438652	XXX		1	456	458226	XX
13	456	439569	XXX		8	444	459737	XX
9	452	440480	XXX		6	443	471775	XX
21	456	441685	XXX		7	444	472111	XX
17	456	442410	XXX		15	456	473732	XX
5	443	44416,	XXX		***11***	***456***	***499786***	***X***

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

CONCLUSIONES

Las siguientes son las conclusiones de la valoración documentada en el presente artículo:

- La caracterización estadística del tráfico de red en condiciones normales es valiosa para crear una línea base de desempeño o estado. Se asume que la construcción de esta línea base se hace en condiciones normales, por lo que es necesario excluir horas de tráfico atípico (domingos, festivos).

- Se encontraron similitudes estadísticas del tráfico de entrada con el tráfico de salida (medias, desviación estándar, máximos, mínimos).

- Todas las pruebas de bondad y ajuste para determinar la normalidad del tráfico resultaron negativas. Tampoco se encontró evidencia de normalidad en el tráfico aislado por horas.

- Todas las pruebas de bondad y ajuste para determinar si el tráfico sigue distribuciones de Fisher, Chi-cuadrado o Erlang resultaron negativas.

- Para el caso estudiado (tráfico de un servidor web) el tráfico por hora, tanto de entrada como de salida, tiene una media y una desviación estándar que puede considerarse estadísticamente invariable en el tiempo. Este hallazgo es el más valioso del presente análisis, puesto que puede utilizarse en la detección de situaciones anómalas o atípicas que sugieren presencia de amenazas o ataques cibernéticos. El análisis permitió establecer que existen horas en las que el tráfico puede variar con respecto a la media; estas pueden ser definidas en el IDS como "horas atípicas" y en las cuales no se espera que el tráfico tenga una media igual a la de las otras horas del día.

La sensibilidad del modelo planteado es baja en el tiempo. Es decir, para ataques de duración de menos de 90 segundos no se detectó un cambio significativo en la estabilidad de las medias, lo cual significa que estos eventos serían imperceptibles para el mecanismo planteado.

- Bajo el modelo propuesto, y como se anotó anteriormente, la detección de una situación en la que la media del tráfico cambia (como en el caso

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

de la simulación de un ataque DoS que satura el enlace de entrada), no es condición suficiente para concluir que se trata de un ataque informático. Otras variables o condiciones como *logs*, banderas de los paquetes y datagramas, origen y destino del tráfico, entre otras, deben revisarse y considerarse para emitir una alarma. Los sistemas de correlación de eventos, por ejemplo, reciben como entrada múltiples fuentes o sensores y emiten alertas cuando relacionan eventos que aislados pueden no indicar ninguna anomalía, pero que en conjunto constituyen evidencia para detectar un ataque o incidente que afecte la seguridad de la información [18].

REFERENCIAS

[1] H.-K. Choi and J. Limb, "A behavioral model of Web traffic", in *Seventh International Confrence on Network Protocols, 1999. (ICNP '99)*, Toronto, Canada, 1999.

[2] S. Ihm and V. S. Pai, "Towards understanding modern web traffic", in *IMC '11 Proceedings of the 2011 ACM SIGCOMM conference*, Berlin, Germany, 2011.

[3] J. Ju-Yeon, K. Yoohwan and K. S. Kyunghee, "Baseline profile stability for network anomaly detection" in *Third International Conference on Information Technology: New Generations, ITNG*, Las Vegas, Nevada, United States, 2006.

[4] H. Hajji, "Statistical analysis of network traffic for adaptive faults detection", *Neural Networks, IEEE Transactions,* vol. 16, n.° 5, pp. 1053-1063, 2005. DOI: 10.1109/TNN.2005.853414

[5] B. Irwin, "A baseline study of potentially malicious activity across five network telescopes", in *2013 5th International Conference Cyber Conflict (CyCon),* pp. 1-17, 2013.

[6] E. Corchado and A. Herrero, "Neural visualization of network traffic data for intrusion detection *RID C-7404-2009*," *Applied Soft Computing,* vol. 11, n.° 2, pp. 2042-2056, #mar# 2011.

[7] R. Vijayasarathy, S. Raghavan and B. Ravindran, "A system approach to network modeling for *DDoS* detection using a Naíve Bayesian classifier", in *Third International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, India, 2011.

[8] R. R. Karthick, V. Hattiwale and B. Ravindran, "Adaptive network intrusion detection system using a hybrid approach", in *Fourth International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, India, 2012.

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)

[9] Microsoft, "Cómo tomarle el pulso a un servidor", Microsoft, [Online]. Disponible en http://technet.microsoft.com/es-es/magazine/2008.08.pulse.aspx.

[10] J. Blommers, *OpenView network node manager: Designing and implementing an enterprise solution,* Prentice Hall Professional, 2000.

[11] Xlstat, "*XLS*tat," Xlstat, [Online]. Disponible en http://www.xlstat.com/es/.

[12] A. Papoulis, *Probability, random variables, and stochastic processes,* New York: McGraw-Hill, 1991.

[13] K. Banks, J. Blackstone, S. Perry, W. Patterson, P. G. des, S. Mujica, C. Aedo, A. Sanchez, J. Andrade and J. Stuardo, "*DDoS* and other anomalous web traffic behavior in selected countries", in *Southeastcon, 2012 Proceedings of IEEE*, Orlando, Florida, United States, 2012.

[14] X. Chen, S. Li, J. Ma and J. Li, "Quantitative threat assessment of denial of service attacks on service availability", in *IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, Shanghai, China, 2011.

[15] B. Devi, G. Preetha and S. Shalinie, "*DDoS* Detection using host-network based metrics and mitigation in experimental testbed", in *International Conference on Recent Trends In Information Technology (ICRTIT)*, Tamil Nadu, India, 2012.

[16] P. Hershey and C. Silio, "Procedure for detection of and response to distributed denial of service cyber attacks on complex enterprise systems", in *IEEE International Systems Conference (SysCon)*, Vancouver, Canada, 2012. DOI: 10.1109/SysCon.2012.6189438

[17] A. Persia, M. Durairaj and S. Sivagowry, "Study of thwarting DoS attacks by detecting *MAC* spoof in *WLAN* infrastructure networks," in *IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, Ramanathapuram, India, 2012.

[18] F. Lan, W. Chunlei and M. Guoqing, "A framework for network security situation awareness based on knowledge discovery" in *Second International Conference on Computer Engineering and Technology (ICCET)*, Chengdu, China, 2010.

ISSN: 0122-3461 (*impreso*)
2145-9371 (*on line*)