Artículo **Revista de Simulación Computacional**

Diciembre 2017 Vol.1 No.2 24-31

Sistema inteligente para validar una lista de control de acceso (ACL) en una red de comunicaciones

HERNANDEZ, Talhia†*, SALAZAR, Pedro, SOTO, Saul

Recibido: 28 de Agosto, 2017; Aceptado 5 de Noviembre, 2017

Resumen

La protección y prevención de la seguridad en redes de comunicación requiere de un método cuidadoso, realista y preventivo en toda organización. Por lo que, los profesionales en el área de administración de redes de comunicaciones deben utilizar nuevas herramientas tecnológicas basadas en estándares nacionales e internacionales que ayuden a mantener la seguridad informática.

El estándar internacional ISO 27002 trata los distintos criterios para las buenas prácticas que ayuden a mejorar la gestión de seguridad de la información en las organizaciones, con base en la implementación de un conjunto adecuado de controles. Las listas de control de acceso (ACL) son un tipo de control que ayuda a definir permisos o accesos según las políticas de seguridad establecidas por la organización y gestionadas por el administrador de la red de comunicaciones.

Por lo anterior, el presente artículo describe el diseño de un sistema inteligente para validar la estructura de una ACL que controle accesos, como lo establece la norma ISO 27002; con la finalidad de que, los expertos en el área lo utilicen como herramienta para la aplicación de las buenas prácticas. Considerando una metodología que consta de las siguientes fases: identificación del problema, identificación de conceptos y datos, adquisición del conocimiento y representación del conocimiento.

Sistema Inteligente, Norma ISO, Seguridad Informática

Abstract

The protection and prevention of security in communication networks requires a careful, realistic and preventive method in any organization. Therefore, professionals in the area of communications network management must use new technological tools based on national and international standards that help maintain computer security.

The international standard ISO 27002 addresses the different criteria for good practices that help improve the management of information security in organizations, based on the implementation of an adequate set of controls. Access control lists (ACLs) are a type of control that helps define permissions or access according to the security policies established by the organization and managed by the administrator of the communications network.

For the above, the present article describes the design of an intelligent system to validate the structure of an ACL that controls accesses, as established by the ISO 27002 standard; With the aim that the experts in the area use it as a tool for the application of good practices. Considering a methodology that consists of the following phases: identification of the problem, identification of concepts and data, acquisition of knowledge and representation of knowledge.

Intelligent System, ISO Standard, Computer Security

Citación: HERNANDEZ, Talhia†*, SALAZAR, Pedro, SOTO, Saul. Sistema inteligente para validar una lista de control de acceso (ACL) en una red de comunicaciones. Revista de Simulación Computacional 2017. 1-2: 24-31

† Investigador contribuyendo como primer autor.

* Correspondencia al autor (email: thernandez@itsoeh.edu.mx)

Introducción

Con base en estudios realizados en el año 2016 por la Unión Internacional de Telecomunicaciones (UIT), organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU) [1], se ha identificado que la tasa de penetración del internet corresponde al 81% en los países desarrollados, 40% en los países en desarrollo y 15% en los países menos adelantados y que el acceso a la información a través de la banda ancha puede ser factor importante para el desarrollo sostenible en el mundo.

A medida que el comercio electrónico y el uso de aplicaciones web sigan creciendo, será difícil encontrar el equilibrio entre estar aislado o abierto a la red de comunicación mundial, internet. Asimismo, la apertura de las redes inalámbricas exige soluciones de seguridad perfectamente integradas, más transparentes y flexibles.

La Organización Internacional para la Estandarización (ISO) ha creado la ISO 27002[2], con enfoque en la "gestión de seguridad de la información mediante la aplicación de controles óptimos a las necesidades de las organizaciones"; por lo que, las Listas de Control de Acceso (ACL) son una alternativa para el control sobre la seguridad en una red de cómputo[3], pero resulta abundante el número de combinaciones posibles que pueden declararse en la entrada o salida de una red, el protocolo, el puerto o servicio que se desea denegar o permitir.

Una ACL es una configuración de router que permite o deniega paquetes según el criterio encontrado en el encabezado del mismo, comúnmente utilizadas en el IOS de Cisco para seleccionar los tipos de tráfico por analizar, reenviar o procesar.

Por lo anterior, el presente artículo da a conocer el diseño de un sistema inteligente con base en experiencias y conocimientos de los administradores de redes de comunicación, para prevenir los accesos no autorizados; utilizando mecanismos conforme a lo que establece la norma ISO 27002, y con ello realizar actividades de fomento y promoción de las buenas prácticas para la aplicación de controles para la seguridad de la información.

El sistema inteligente valida la estructura de una ACL estándar considerando los siguientes datos: Nombre, Acción (Permitir/ Denegar), Dirección IP (Internet Protocol), Protocolo o Servicio; los cuales son definidos en la configuración del router.

La metodología general de diseño del sistema inteligente se basa en las etapas de [4]: identificación del problema, identificación de conceptos y datos, adquisición del conocimiento, representación del conocimiento.

Estado del arte

La seguridad de la información hoy en día en las organizaciones públicas y privadas es un punto de atención [5], además impacta al desempeño e imagen de la misma a partir de verse afectada por ataques de seguridad, esto repercute de forma directa a las operaciones del día a día y del grado de competitividad dentro del sector de mercado al que pertenece.

En la iniciativa privada, con el propósito de ayudar a las organizaciones en cómo prevenir ataques de seguridad que afecten su infraestructura, aplicaciones y servicios, existen distintos estándares a nivel internacional; sin embargo, uno de los más importantes es el creado por la Organización de Estándares Internacionales (ISO).

ISSN 2523-6865

La norma ISO 27002 [6] está teniendo año con año mayor grado de reconocimiento y adopción; por ser un lenguaje común de las organizaciones a lo largo de todo el mundo para la seguridad de información [7].

La versión 2013 de esta norma [8], trata acerca de la continuidad de la seguridad de la información embebida en un "Sistema de Gestión de Continuidad de los Negocios (SGCN)", estableciendo en la cláusula 9 "Control de Acceso: los requisitos de la organización para controlar el acceso a los activos de información deben estar claramente documentados en una política y procedimientos de control de acceso".

Para ello, la propuesta de implementación de un sistema inteligente [9] en la organización, ayuda a las personas en el análisis de problemas y la toma de decisiones para el diagnóstico del nivel de seguridad otorgado por un procedimiento de control de acceso con mayor rapidez y eficacia, como si lo hiciera un humano experto en el área.

En el año 2011 investigadores de la Universidad Interamericana de Puerto Rico [10], realizaron una investigación para determinar si los sistemas inteligentes son una solución viable para identificar y prevenir las vulnerabilidades y riesgos en los sistemas de información de las organizaciones, basándose en 8 elementos para desarrollarlo: organización, planificación, inventario, operaciones, desarrollo y mantenimiento, bitácoras, planificación de contingencias, seguridad; como resultado, se comprobó la hipótesis "los sistemas inteligentes son viables para identificar y prevenir vulnerabilidades".

Sin embargo, está ausente la adopción de una norma o estándar que establezca requisitos para la implementación de las buenas prácticas en temas de seguridad informática.

Al realizar el estado de arte, se encontró una propuesta con la misma finalidad del presente trabajo: mantener la seguridad en la red de comunicaciones usando un sistema experto.

Sin embargo, dicha propuesta consiste en detectar intrusos basado en un sistema experto [21] cuyo objetivo es "detectar un intruso que evadió los mecanismos de seguridad de una red y que llega a un host que no cuenta con un mecanismo de seguridad adicional para su protección", utilizando NACs (Network Access Control) para el control de acceso a la red por medio de cumplimiento de políticas establecidas por propietarios de sistemas a proteger y el sistema experto extrae la aplicación de las reglas generando una conclusión que determina si se trata o no de una intrusión.

Diseño del sistema inteligente para para validar la estructura de una ACL

Con base en una metodología de diseño de sistemas inteligentes, se han considerado algunas etapas, como se muestra en la figura 1.

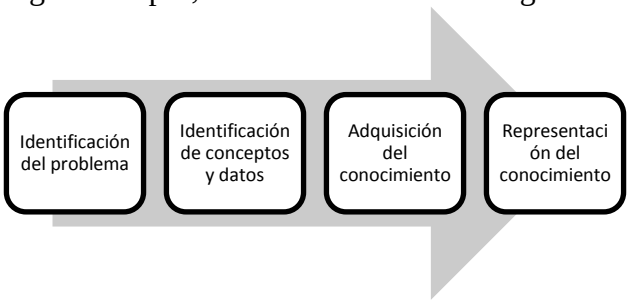

Figura 1 Etapas para el diseño del sistema inteligente.

Para cada etapa se desarrollaron actividades específicas, descritas a continuación:

Descripción del problema

A lo largo de los últimos años se ha visto un incremento en los ataques a las organizaciones.

Por ejemplo, en el primer trimestre del año 2016 se realizó el mayor ataque de negación de servicio [11] (DDoS) "attacks aim at rapidly exhausting the communication and computational power of a network target by flooding it with large volumes of malicious traffic", con un record de 500 Gbps según la firma ARBOR Networks, líder en la solución en ataques este tipo, [12] en su 11° Informe Anual de Infraestructura de Seguridad en todo el mundo, asegura que esto no es un sorpresa, ya que se observa una tendencia de incremento en un 60%; además de resaltar que el 93% de estos ataques se orientan a la capa de aplicación, señalada como una de las siete capas en Modelo de Interconexión de Sistemas Abierto (OSI) de la Organización de Estándares Internacional (OSI), el porcentaje de ataques a los principales protocolos son los siguientes: 84% DNS, 77% NTP, 42% SSDP y 41% SNMP.

El nivel de complejidad de los ataques a las organizaciones ha evolucionado al grado de impactar la infraestructura, aplicaciones y servicios de forma simultánea, en lo que se está denominando ataques 'multi-vecto'. Como una respuesta para mitigar los ataques las organizaciones están implementando principalmente Sistemas de Mitigación de DDoS Inteligentes (IDMS) seguido muy de cerca el uso de Listas de Control de Acceso (ACL), estas últimas son [13] "provides security for a private network by controlling the flow of incoming and outgoing packets. Specifically, a network policy is created in the form of a sequence of (possibly conflicting) rules." señalado por Liu y Torng, habrá que destacar que los principales puertos objetivos de ataques:

- Port 80 con 45.7%
- Port 53 con 12%
- Port 443 con 6.9%
- Port 3074 con 2.3%
- Port 25565 con 2.0%

Identificación de conceptos y datos

Existen 2 tipos de listas de control de acceso: estándar (para el control de directorios y ficheros) y extendida (incluye más elementos), figura 2. Para el diseño del sistema inteligente se ha considerado la validación de las ACL estándar como primera fase, posteriormente se incluirá la validación para las ACL extendidas.

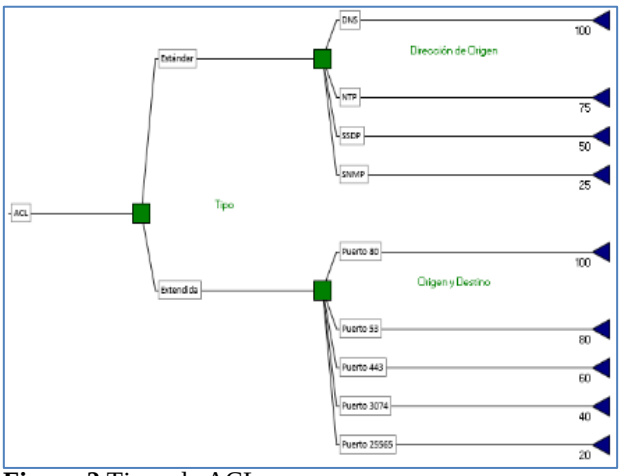

Figura 2 Tipos de ACL.

Con base en la problemática identificada en relación a los de ataques por medio de los principales protocolos, se han definido en la Tabla 1 niveles de riesgo para los 4 primeros protocolos de comunicación con mayor vulnerabilidad:

Protocolo	Nivel de riesgo	Porcentaje
DNS	Muy Alto	100%
NTP	Alto	75%
SSDP	Medio	50%
SNMP	Bajo	25%

Tabla 1 Protocolos con mayor vulnerabilidad**.**

Adquisición del conocimiento

En esta etapa se ha considerado la experiencia y conocimiento de expertos en el área de administración de redes con certificación en CCNA Industrial de CISCO, encargados de las implementaciones y soluciones de problemas comunes de los protocolos estándares en la industria. Por lo tanto, se determinó que el sistema inteligente es funcional para la evaluación de las ACL estándar, a partir de los 4 elementos que la componen: Nombre, Acción (permitir/denegar acceso), Dirección IP y Protocolo, como se muestra en la figura 3.

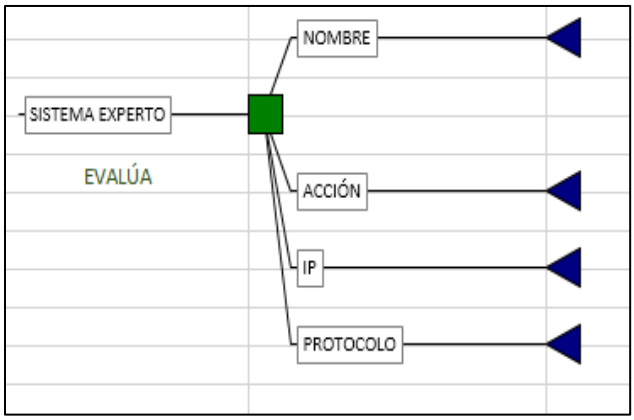

Figura 3 Elementos que componen la ACL estándar.

Representación del conocimiento

Con base en los 4 elementos de la ACL estándar, se han diseñado árboles de decisión para establecer el proceso que debe seguir el sistema inteligente en la validación de la estructura de una ACL estándar, como mecanismo de control para las buenas prácticas sobre la seguridad de la información en las redes de cómputo.

La validez del Nombre de la ACL se otorga a partir de que esté formado por un conjunto de caracteres y números, donde el tamaño de los caracteres es de máximo 32 y los números estarán en el intervalo del 1 al 99 (figura 4)

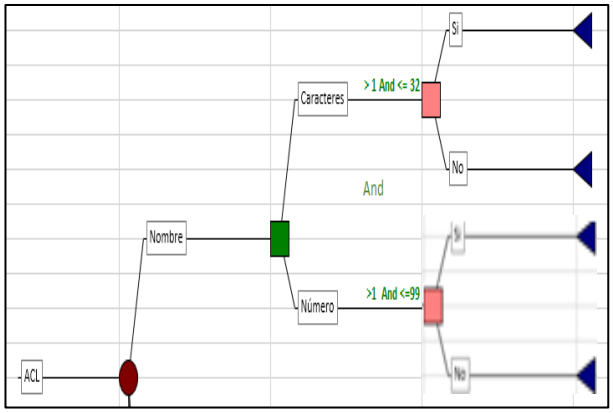

Figura 4 Restricciones para evaluar el nombre de la ACL estándar.

Para evaluar la Acción de la ACL, únicamente se tienen 2 valores “Permit”, para otorgar acceso a la red, en caso contrario “Deny” para denegar la entrada (figura 5).

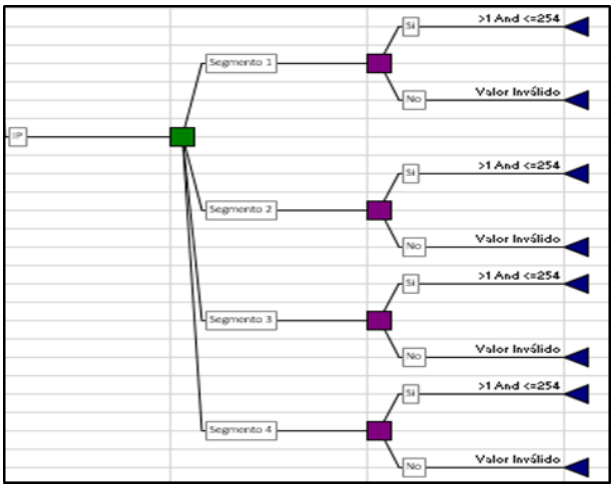

Figura 5 Restricciones para evaluar la acción de la ACL estándar.

Para evaluar la Dirección IP de la ACL, se ha considerado la segmentación de la dirección en cuatro, como se muestra en la figura 6.

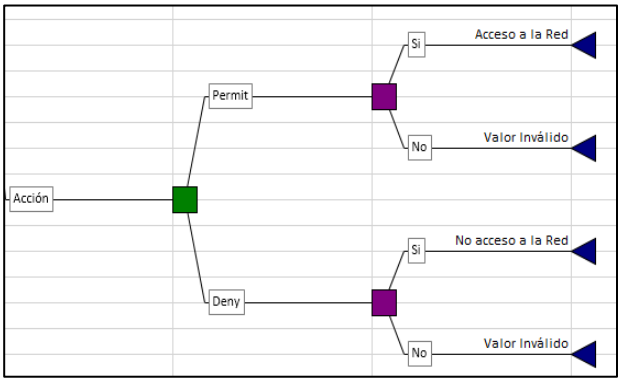

Figura 6 Restricciones para evaluar la dirección IP de la ACL estándar.

Por último, se evalúa el Protocolo que proporciona cierto nivel de riesgo en la red de comunicaciones, para lo cual se han identificado y clasificado lo más comunes. Para cada uno se ha determinado un nivel de riesgo específico, como se muestra en la figura 7.

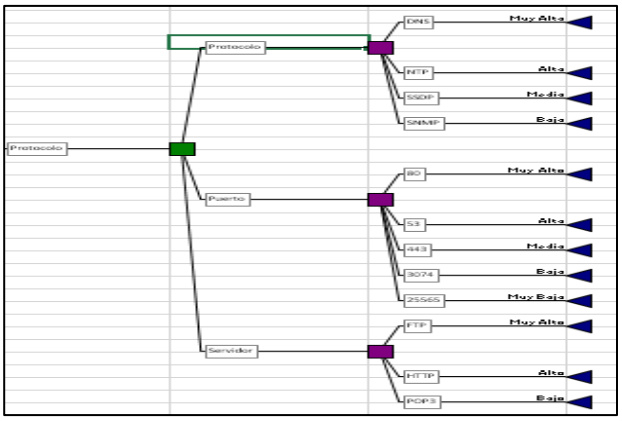

Figura 7 Restricciones para evaluar el nivel de riesgo del protocolo de la ACL estándar.

La figura 8, muestra la prueba de una parte de la base de conocimientos, diseñada para evaluar el nivel de riesgo de los protocolos: DNS, NTP, SSDP, SNMP, que puedan estar definidos en la ACL.

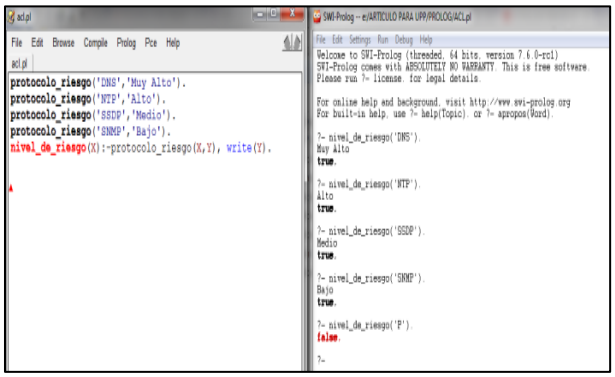

Figura 8 Predicados de la base de conocimientos en PROLOG.

Conclusiones y trabajos futuros

A partir de los conocimientos adquiridos por medio de los expertos en la administración de las redes de cómputo, se ha logrado el diseño lógico de un sistema inteligente que pueda validar una Lista de Control de Acceso (ACL) estándar, antes de que esta sea ingresada a través del router.

El prototipo del sistema inteligente se está desarrollando en el lenguaje PROLOG para la ejecución de las reglas de validación accediendo a la base de conocimiento; sin embargo, para la presentación de resultados se considera realizar una conexión con Java para ofrecer al usuario final (administrador de la red de cómputo) una interfaz gráfica que permita el ingreso de la ACL para ser evaluada por la base de conocimientos.

En lo sucesivo, se presentarán los resultados que arroja la implementación del sistema inteligente; puesto que, aún se encuentra en etapa de desarrollo del programa.

ISSN 2523-6865

Asimismo, en una primera fase del proyecto se ha propuesto la validación de una ACL estándar con base en los 4 elementos que la conforman; sin embargo, se incluirá la validación de una ACL extendida, con la finalidad de realizar las pruebas del sistema inteligente final en un clúster de alta disponibilidad, el cual, aloja aplicaciones web en el ámbito gubernamental y que requiere de la implementación de la norma ISO 27002 para el cumplimiento de la cláusula 9.4 "control de acceso de sistemas y aplicaciones".

Referencias

[1] La UIT pública las cifras de 2016 de las TIC. (2016). Itu.int. Retrieved 22 julio 2016, from http://www.itu.int/es/mediacentre/Pages/2016-PR30.aspx

[2] Ormella, C. (2014). Las nuevas versions de las normas ISO 27001 e ISO 27002. 16 de enero de 2014. Website: http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf

[3] Uhrig, M. N. (2013). Listas de Control de Acceso.

[4] Amador Hidalgo, L. (1996). Inteligencia artificial y sistemas expertos. Universidad de Córdoba, Servicio de Publicaciones.

[5] A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards, Constantine Gikas Information Security Journal: A Global Perspective, Vol. 19, Iss. 3, 2010

[6] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," Journal of Information Security, Vol. 4 No. 2, 2013, pp. 92-100. doi: 10.4236/jis.2013.42011.

[7] E. Humphreys, "Information Security Management System Standards," Datenschutz and Datensicherheit, Vol. 35, No. 1, 2011, pp. 7-11. doi:10.1007/s11623-011-0004-3

[8] ISO 27001 (2017). Retrieved 1 de junio 2017, from http://www.iso27001security.com/html/27002.html#Contents

[9] Harmon, P., & King, D. (1988). Sistemas expertos: aplicaciones de la inteligencia artificial en la actividad empresarial. Ediciones Díaz de Santos.

[10] Cruz, N. E., & Metropolitano, R. (2011). El Rol y Contribución de los Sistemas Expertos en la Prevención de Vulnerabilidades y Riesgos en las Redes y Estaciones de Trabajo.

[11] Gulisano, V., Callau-Zori, M., Fu, Z., Jiménez-Peris, R., Papatriantafilou, M., & PatiñoMartínez, M. (2015). STONE: A streaming DDoS defense framework. Expert Systems With Applications, 42(24), 9620-9633. doi:10.1016/j.eswa.2015.07.027

[12] Annual Security Report. Retrieved July 5, 2016 from https://www.arbornetworks.com/report-thank-you

[13] Liu, A. X., Torng, E., & Meiners, C. R. (2011). Compressing Network Access Control Lists. IEEE Transactions On Parallel & Distributed Systems, 22(12), 1969-1977. doi:10.1109/TPDS.2011.114

[14] Badaró, Sebastián; Ibañez, Leonardo Javier; Agüero, Martín. Sistemas expertos: fundamentos, metodologías y aplicaciones. Ciencia y Tecnología, 2013, vol. 1, no 13

ISSN 2523-6865

[15] W. Boehmer, "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001," 2008 Second International Conference on Emerging Security Information, Systems and Technologies, Cap Esterel, 2008, pp. 224-231. doi: 10.1109/SECURWARE.2008.7

[16] Esmoris, D. O. (2010). Control de acceso a redes (Doctoral dissertation, Facultad de Informática).

[17] Matturro, G. (2007). Introducción a la Configuración de Routers Cisco.

[18] Castillo, G. G., Trejo, E. R., & de León, H. MONITOREO Y CONTROL EN UNA RED POR MEDIO DE VISUALIZADORES DE PAQUETES IPv4/IPv6 Y LISTAS DE ACCESO DE UN ROUTER.

[19] Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., & Weippl, E. (2007, December). Information security fortification by ontological mapping of the ISO/IEC 27001 standard. In Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on (pp. 381-388). IEEE.

[20] Bueno Rosales, J. J. (2013). Sistema de control y seguridad endian Firewall para la empresa Frada Sport (Bachelor's thesis, Quito: Universidad Israel, 2013).

[21] Márquez, V. E. G., Sistema de detección de intrusos basado en sistema experto, in Centro de Investigación en Computación, Instituto Politécnico Nacional, México, pp. 78-79 (2010).

ISSN 2523-6865