Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS

Implementation of a computer perimeter security system using VPN, firewall and IDS

John Jaime Marín Valencia[1]
Alejandro Patiño Valencia[2]
Juan Camilo Acevedo Bedoya[3]

1 Ingeniero electrónico, consultor junior, Newsoft S. A. S. (Rionegro, Antioquia, Colombia). Correo electrónico: jjmarinva10@gmail.com.

2 Ingeniero electrónico, consultor de software, Accenture (Rionegro, Antioquia, Colombia). Correo electrónico: alejin099@hotmail.com.

3 Especialista en Seguridad Informática, grupo de investigación GIMU; docente de tiempo completo, Facultad de Ingenierías, Universidad Católica de Oriente (Rionegro, Antioquia, Colombia). Correo electrónico: jacevedo@uco.edu.co.

Cómo citar este artículo:
Marín Valencia, J. J.; Patiño Valencia, A. & Acevedo Bedoya, J. C. (2020). Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS. *Revista Universidad Católica de Oriente, 31*(45), 84-99.

Resumen

En este artículo se presenta la implementación de un sistema de seguridad perimetral informático que contiene los servicios de una red privada virtual, un cortafuegos y un sistema de detección de intrusos. La integración e implementación de dichos servicios permite mejorar la seguridad de una red del tamaño de una microempresa, ya que el sistema se encarga de mitigar posibles ataques que buscan penetrar y vulnerar los sistemas de seguridad establecidos por una empresa. Para probar el sistema se hizo indispensable realizar pruebas técnicas de penetración mediante la distribución Kali del sistema operativo Linux. Posteriormente, cuando se realizó la prueba integral del sistema, se concluyó que este neutralizaba los ataques de denegación de servicios y ataques de fuerza bruta de manera esperada, siempre y cuando los escudos de seguridad y las reglas definidas por el administrador de la red estuvieran activas. Además, también se requería que el usuario hiciera uso de las herramientas desarrolladas, por esta misma razón es que se hace indispensable la concientización del personal corporativo en temas de seguridad, puesto que la base de la seguridad informática parte desde el interior hacia el exterior.

Palabras clave

VPN, *firewall*, IDS, ciberataques, ataques de fuerza bruta.

Abstract

This paper shows the implementation of a computer perimeter security system that contains the services of a virtual private network, a firewall, and an intrusion detection system. The integration and implementation of these services allows improving the security of a network the size of a microenterprise, since the system is responsible for mitigating possible attacks that seek to penetrate and break the security systems established by a company. To test the system, it was essential to perform technical penetration tests using the Kali distribution of the Linux operating system. Later, when the system was fully tested, it was concluded that the system neutralized denial of service attacks and brute force attacks in an expected manner as long as the security shields and the rules defined by the administrator of the network were active. In addition, it was also required that the user made use of the tools developed, for this same reason is that it is essential to raise awareness of corporate personnel on security issues, since the basis of computer security starts from the inside to the outside.

Key words

VPN, firewall, IDS, cyber attacks, brute force attacks.

Intoducción

Las redes de datos han evolucionado a tal punto, que cualquier persona puede acceder a la información desde cualquier parte a través de internet, gracias a esto es posible trabajar desde cualquier lugar. Sin embargo, la inseguridad a la que se expone de la información ha venido incrementado desde hace algunos años porque «la cantidad de dispositivos que se conectan a la red, no poseen un protocolo de seguridad estándar y seguro» (Camacho Torrens, 2018). Este tipo de vulnerabilidades hacen que dichos dispositivos sean blanco objetivo de los *hackers*. Por esta razón es que en los últimos años se ha venido evidenciado que ocurren más de 4000 ataques por día (Estados Unidos, 2018), dentro de los cuales se destaca el famoso ataque del *ransomware* Petwrap que ocurrió el 27 de junio del año 2017 (Furnell y Emm, 2017).

Así mismo, en Colombia al mes:

> Se registran alrededor de 187 denuncias por robos informáticos, los más comunes a través de la modalidad de *phishing* (pesca de información), que es un delito digital en el que, por medio de correos electrónicos, se engaña a las personas para que entreguen información como claves bancarias, número de cedula, contraseñas y realicen movimientos financieros (Unilibre, 2019).

Otro caso similar reportó la compañía de seguridad informática Kaspersky (González, 2017), donde se afirma que: «Los ataques e infecciones de *ransomware* están creciendo a un ritmo alarmante y se han convertido en el tipo de amenaza más prominente» (Thomas, 2018). Además, «el *phishing* o extracción fraudulenta de información de las personas es uno de los delitos cibernéticos con cifras más alarmantes» (El Mundo, 2017). Según Kaspersky, «solo en diciembre de 2016 la cifra de casos de *phishing* aumentó en un 22,6 % comparado con el año 2015 en Colombia». Así mismo, se reciben cerca de 200 denuncias mensuales y la empresa de seguridad RSA señala que: «Los ataques cibernéticos aumentan entre un 30 % y un 40 % cada año» (Farro, Flores, 2017).

Es por esto por lo que se ha observado el surgir de nuevos sistemas de seguridad conforme a las nuevas vulnerabilidades halladas por los *hackers*. No obstante, al ser un tema importante genera unos costos considerables asociados a la prevención de los ataques, costos computacionales y las pérdidas como consecuencia de estos. Por esto se implementó un sistema de seguridad perimetral que puede ser una solución viable para todas las empresas que no posean grandes recursos económicos, ya que el principal objetivo es ofrecer una

solución a bajo costo que permita a las compañías mitigar el riesgo de sufrir un ataque de seguridad informática, esto con el fin de mejorar la confidencialidad, disponibilidad e integridad de la información. Es decir, que la información viaje de un lugar a otro sin ser modificada o interceptada por una tercera parte, a su vez que esté disponible en cualquier momento y que solo pueda ser observada por el emisor y receptor.

El sistema implementado cuenta con los servicios de una VPN, *firewall* e IDS, ya que actualmente en el mercado no se encontró un sistema que incorpore estos tres servicios. A continuación, se presenta una descripción de los servicios que el sistema mencionado posee, y con los cuales se piensa mejorar la seguridad de una microempresa.

Red privada virtual (VPN)

Es una tecnología que generalmente puede ser una red para estudiantes o para administración. Además, permite conectarse a un lugar remoto por medio de una red pública que generalmente es internet. «Algunas empresas suelen utilizar estas redes para que los empleados puedan acceder a recursos corporativos de una manera segura» (ESET Security, 2017). Una de las grandes ventajas de este tipo de arquitectura son la confidencialidad e integridad de la información, puesto que se genera un canal cifrado por donde pasarán los datos, dándole así una mayor seguridad a la información.

Firewall

Es un servicio que permite filtrar información, a través del monitoreo constante del contenido entrante en la red, donde de acuerdo con las políticas establecidas por la compañía se decide si se bloquea o permite el tráfico. Para el sistema desarrollado el *firewall* será un filtro que protegerá a la red local del tráfico externo no deseado.

Sistema de detección de intrusos (IDS)

«Es un mecanismo que permite identificar tráfico y notificar al administrador de red, con el fin de mitigar el riesgo de sufrir un ataque informático o de revelar información que comprometa la seguridad de la compañía» (Sánchez, 2004). Puesto que, acorde a la literatura, se ha identificado que muchos de los ataques informáticos provienen desde la red interna, el IDS permitirá identificar y notificar el tipo de tráfico presente en la red local.

Metodología

En la Figura 1 se presenta un diagrama de bloques general de cada una de las etapas seguidas en el desarrollo de este trabajo. Inicialmente, se realizó un proceso de análisis para la utilización del tipo de *hardware* idóneo y herramientas existentes para implementar un servidor VPN, *firewall* e IDS; posteriormente, se procede a desarrollar cada uno de los servicios descritos; en tercer lugar, se implementa un solo sistema, el cual contiene los tres servicios que son: servidor VPN, *firewall* e IDS.

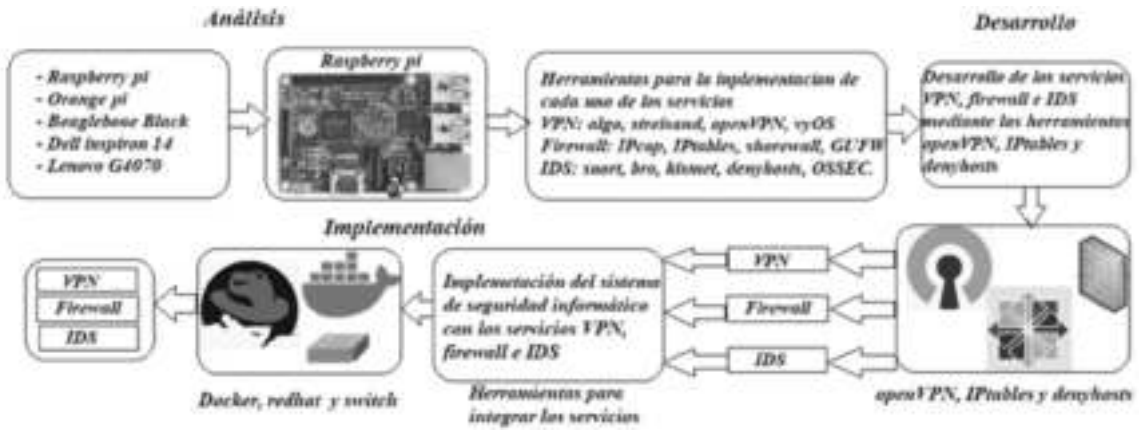

Figura 1. Diagrama de bloques de la metodología propuesta. Fuente: Elaboración propia.

Se procede a describir los pasos que se siguieron en el desarrollo metodológico:

Análisis del problema

En esta fase se hace un análisis de los diferentes tipos de herramientas *open source*, que se ofrecen en los sistemas operativos de distribución basados en Linux para desarrollar una VPN, *firewall* e IDS, posterior a esto, se evalúan los tipos de ordenadores de placa reducida para determinar el que mejor se ajuste a la implementación del IPS.

Desarrollo

Para el servicio del *firewall* se desarrolló un aplicativo en Java que permite a los usuarios, que no tienen conocimientos técnicos en redes, establecer políticas de seguridad tales como: permitir o denegar un *host* remoto, comprobar el estado de la comunicación del *host* local con uno o varios equipos remotos de una red IP, a través del protocolo de control de mensajes de internet (ICMP), denegar o permitir un dominio, evitar o permitir acceso a internet a varios *hosts* dentro de la red LAN, denegar o permitir *ping* por medio de la dirección MAC del *host* definido en la interfaz gráfica.

Además, el sistema cuenta con unos escudos de seguridad que vienen establecidos por defecto con la finalidad de proteger a los usuarios de la red local de los siguientes ataques:

Ataques DDOS: consiste en realizar peticiones de manera masiva a un servidor, con el fin de saturarlo e inhabilitarlo temporalmente.

Inundación de SynFlood: es una variante de un ataque de DDOS que explota las vulnerabilidades del servidor víctima, enviando peticiones SYN a través de diferentes puertos por medio de direcciones IP falsas.

Ataques de fuerza bruta: se encargan de entrar al sistema mediante la realización de combinaciones masivas de usuario y contraseña; estas credenciales generalmente vienen vinculadas a los dispositivos por configuración de fábrica.

Para la implementación del *firewall* se usó la utilidad Iptables, la cual es una herramienta del kernel de Linux. En la Figura 2 se muestra la interfaz desarrollada, mediante la cual un usuario podrá establecer las políticas de seguridad informática anteriormente descritas.

Figura 2. Interfaz de configuración para el firewall.
Fuente: Elaboración propia.

Para la implementación del servidor VPN se hizo necesario realizar una apertura de puertos en el Router Arris TG862, proporcionado por el proveedor de servicios de internet (IPS), Claro. Teniendo la topología de red lista, se hace uso de la herramienta Openvpn, que sirve para implementar un servidor VPN, mediante el protocolo de seguridad IPs, con cifrado simétrico AES.

Luego de tener implementado el servicio VPN se migró a un contenedor Docker, el cual es una forma de poder ejecutarlo en cualquier SO. Otra de las ventajas de tener el servidor VPN dentro de un contenedor Docker, es darle más escalabilidad a la red, permitiendo mediante la herramienta Docker Swarm, implementar técnicas de computación paralela.

Finalmente, para la implementación del sistema de detección de intrusos, se hizo uso de la herramienta Denyhosts, que es nativa de Linux y permite establecer parámetros como el número de intentos erróneos al intentar acceder al sistema haciendo de esta una eficaz herramienta frente a los ataques de fuerza bruta. Además, se puede configurar el tiempo máximo para el cual el *host* atacante puede estar conectado. Por lo tanto, el sistema cuenta con notificaciones en tiempo real, a través de correo electrónico, con información del *host* atacante.

Implementación

El sistema se implementó en una Raspberry Pi B con SO Raspbian. Se hizo uso del enrutador proporcionado por el proveedor de internet para el ingreso al servidor VPN. Como equipos clientes se usaron dos portátiles, mientras que para la prueba del firewall e IDS se usaron dos celulares y un portátil. En la Figura 3 se muestra la topología de red implementada para el IPS.

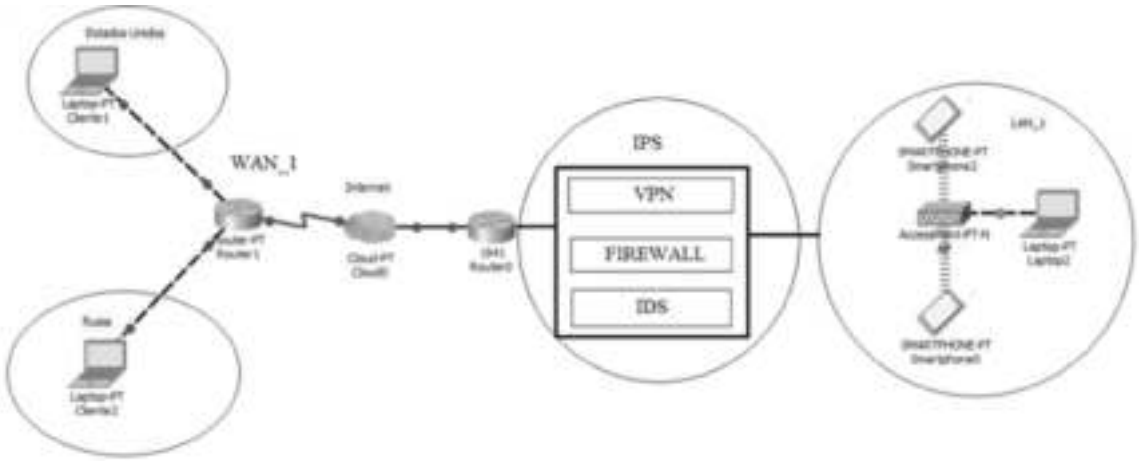

Figura 3. Topología de red del IPS.
Fuente: Elaboración propia.

Resultados

El sistema implementado se puso a prueba durante ocho horas continuas, en las cuales se realizaron diversos ataques de penetración mediante la distribución de Linux Kali, con el apoyo de ocho máquinas zombi. Durante el periodo de prueba se evidenció cómo el sistema contenía cada uno de los ataques, realizando acciones tanto preventivas como correctivas, dependiendo del ataque generado. A continuación, se muestran cada uno de los ataques generados.

Ataque DDOS mediante ping de la muerte

Para simular este ataque se tomaron cinco máquinas zombis, las cuales realizaban peticiones constantes al servidor con el fin de saturarlo. Para la contención de estos ataques se definieron varias reglas:

```
iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

Donde:

Limit 25/minute: limita a solo 25 conexiones por minuto.

Limit-burst 100: indica que el valor de limit/minute será forzado solo después del número de conexiones en este nivel.

Esta regla permite al sistema detectar y ejecutar una acción una vez se sobrepase el límite establecido en la regla. Cuando se llega al tope establecido, se comienzan a abortar conexiones de manera controlada, ya que no se deniega el protocolo ICMP por completo, que es una de las alternativas con las que se cuenta. En la Figura 4 se puede observar una solicitud de *ping* que es enviada desde un *host* local a todo el servidor.

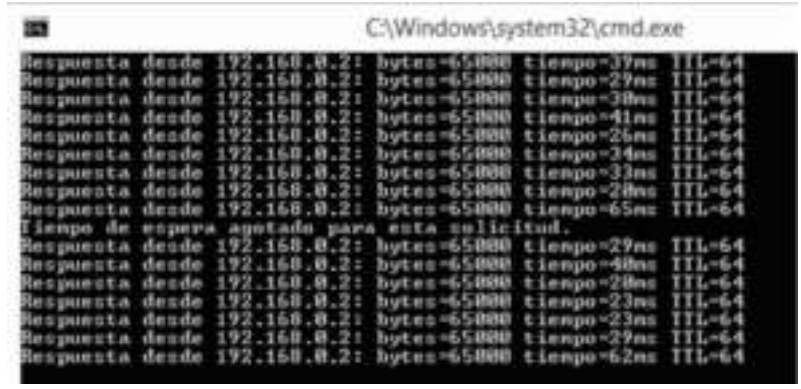

Figura 4. Ping de la muerte de 65000 bytes de longitud.
Fuente: Elaboración propia.

También se evidenció, a través de los ataques generados con los equipos de cómputo que simula una pequeña empresa, que el rendimiento del servidor en la Raspberry Pi no se vio afectado, puesto que cuando se intentó acceder a este, a través de una conexión remota por un canal cifrado, además de acceder a recursos de este servidor y navegar por medio de internet, trabajó satisfactoriamente como era lo esperado.

Ataque de inundación SYN

Este tipo de ataque fue simulado con la instrucción hping3 192.168.1.24 -p 80 –fast, proporcionado por la herramienta Kali, obteniéndose como resultado la respuesta que se muestra en la Figura 5.

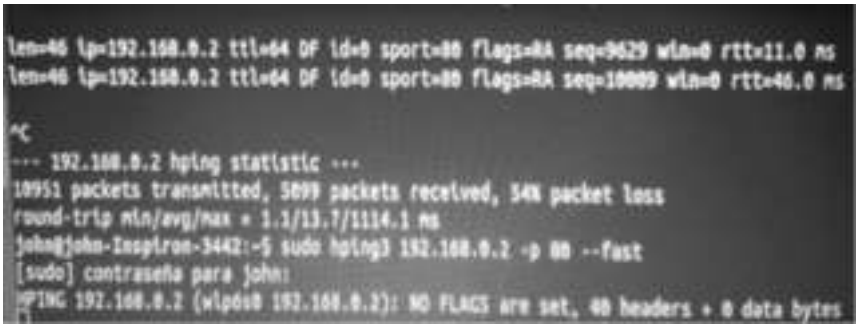

Figura 5. Respuesta al ataque de inundación SYN.
Fuente: Elaboración propia.

Inicialmente, el sistema comenzó a responder las peticiones del *host* atacante, pero una vez se detecta que se trataba de un posible ataque, el sistema aborta la conexión y termina las solicitudes.

En la Figura 6 se puede observar un ataque, el cual es detectado por el Sniffer Wireshark desde un *host* local que tiene como dirección IP 192.168.0.24.

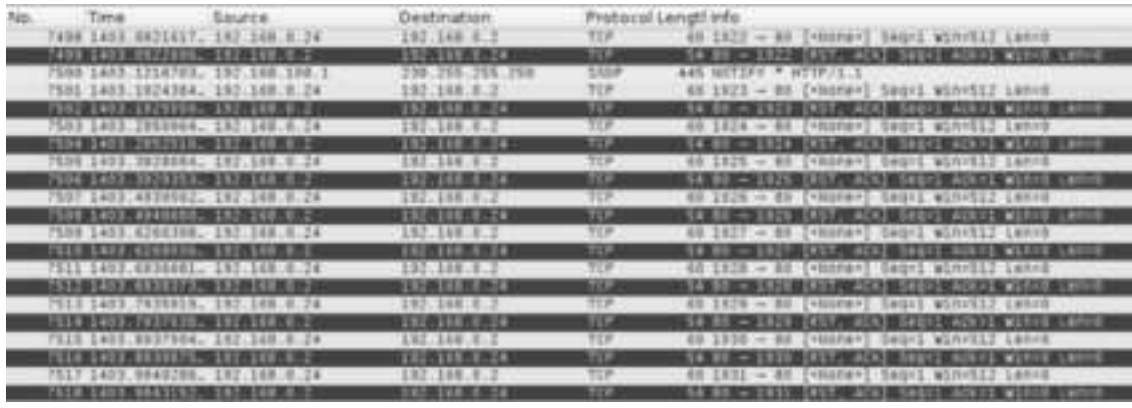

Figura 6. Inundación de SYN *vista en el servidor mediante el Sniffer Wireshark. Fuente: Elaboración propia.*

Ataque fuerza bruta

Para la realización de este ataque se inicializó varias veces con credenciales que vienen asociadas por defecto por los fabricantes de los dispositivos, con la finalidad de intentar romper y abrir una brecha de seguridad, para luego acceder a los recursos del servidor. Se evidenció que tan pronto el atacante erraba tres combinaciones de usuario y contraseña, el sistema bloqueaba el acceso por una semana y enviaba una notificación en tiempo real a los correos electrónicos de los administradores. De igual forma, dentro del servidor se generaba un archivo de texto con el reporte de la dirección IP. Las siguientes líneas son parte del reporte generado por el ataque:

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.

# DenyHosts: Fri Mar 8 17:04:11 2019 | sshd: 192.168.0.11

sshd: 192.168.0.11

# DenyHosts: Fri Mar 8 17:04:11 2019 | sshd: 192.168.0.28

sshd: 192.168.0.28

# DenyHosts: Fri Mar 8 17:04:11 2019 | sshd: 192.168.0.60

sshd: 192.168.0.60
```

En la Figura 7 se muestra la notificación de correo electrónico enviada por el sistema.

Figura 7. Notificación en tiempo real al ataque de fuerza bruta. Fuente: Elaboración propia.

El funcionamiento del servidor VPN se validó mediante el software de emulación de terminal PuTTY. En la Figura 8 se observan los parámetros para el ingreso al servidor VPN desde una ubicación remota. Se muestra la dirección IP usada por el servidor VPN y el protocolo SSH, para un acceso por consola segura.

Figura 8. Ingreso de datos en el software PuTTY. Fuente: Elaboración propia.

En la Figura 9 se puede observar la conexión al servidor VPN de un cliente de forma remota mediante el protocolo SSH. En esta conexión se puede acceder a los recursos del servidor, ejecutar comandos, además de conectarse a internet evitando censuras a páginas que dictan algunos países.

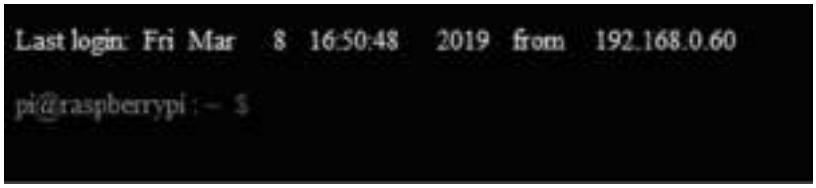

Figura 9. Ingreso al servidor VPN. Fuente: Elaboración propia.

El tipo de arquitectura de *hardware* idónea se definió como aquel sistema que presentó una relación costo beneficio favorable, además de cumplir con ciertas características técnicas dentro de los cuales se destacaron: la unidad central de procesamiento CPU, la memoria de acceso aleatorio RAM y las interfaces de red. Posterior a ello se realizó un *benchmarking*, que consiste en realizar un análisis de rendimiento del ordenador, lo que genera un informe que detalla un resumen de las características del equipo analizado. En la Tabla 1 se muestran los atributos de interés.

Considerando los reportes generados, se concluyó que el *hardware* que más se adecuaba a las necesidades del sistema a implementar era un ordenador de placa reducida con referencia Raspberry pi 3B, cuyo precio oscilaba en el mercado entre $100 000 y $200 000. Luego, se procedió a adquirir dicho ordenador de placa reducida.

Tabla 1. Comparativa de hardware entre ordenadores.

Referencia	Precio	CPU	RAM	Interfaces de red
Raspberry Pi 3B	$165 000	1.4GHz 64-bit quad-core ARM Cortex-A53 CPU	1GB LPDDR2 (900 MHz)	2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE. Gigabit Ethernet over USB 2.0 (maximum throughput 300 Mbps)
Orange pi 2	$100 000	H3 Quad-core Cortex-A7 H.265/HEVC 4K. GPU	1GB DDR3	10/100/1000M Ethernet RJ45 WiFi: Realtek RTL8189ETV, IEEE 802.11 b/g/n

Lenovo G4070	$1 300 000	Intel(R) Core (TM) i5-4200U CPU @ 1.60GHz (4 CPUs), ~1.6GHz	4 RAM	Realtek RTL8723BE Wireless LAN 802.11n PCI-E NIC. LAN 10 / 100 Mbps
Dell Inspiron 14	$1 300 000	Intel(R) Core (TM) i5-4210U CPU @ 1.70GHz (4 CPUs), ~1.7GHz	4 RAM	10/100/1000M Ethernet RJ45. Dell Wireless 1704 802.11b/n (2,4GHz)
Beagalebone Black	$263 000	AM3358BZCZ100 Cortex A8 ARM	512MB DDR3 RAM	10/100 ETHERNET. RJ45

Fuente: Elaboración propia.

Conclusiones

Después de implementar el sistema de seguridad perimetral y realizar las pruebas integrales, se observó que el sistema puede mejorar la seguridad de una red local pequeña de manera satisfactoria. No obstante, como trabajo futuro se propone complementar el sistema con un servidor proxy que permita establecer listas de control de acceso (ACLs), las cuales posibilitarían que el administrador de la red tenga un mejor control de esta. De igual manera, se debe garantizar la generación de *logs* que registren la actividad de la red a nivel de la capa de aplicación, para posteriormente extraer reportes y generar un análisis del estado actual de la red, y en un futuro cercano establecer mejores prácticas de seguridad.

La estabilidad de la red LAN inalámbrica generada fue evaluada en dos ambientes, el primero de ellos encerrado y con poca presencia de señales WiFi, y el otro en presencia de dichas señales, lo anterior permitió concluir que en presencia de ondas electromagnéticas de 2.4 GHz el sistema AP se comporta de manera inestable, por lo que se hace indispensable antes de iniciar la Raspberry como punto de acceso, asignar un canal que esté libre de interferencia, es decir, que se debe verificar la disponibilidad de estos, ya que dependiendo de esta configuración se tendrá la estabilidad de la red generada.

Después de realizar los ataques de penetración más comunes a través de la distribución Kali de Linux, se concluye que el sistema responde de manera eficiente a los tipos de amenazas más comunes, es decir, que con el sistema desarrollado se pueden mitigar los riesgos que en la pequeña empresa o firma se puedan presentar.

La combinación entre un *firewall* y un IDS hace que el sistema sea robusto, puesto que mientras uno de los sistemas identifica una posible amenaza, el otro sistema ejecuta una acción para mitigar el posible ataque, esto es indispensable para establecer un análisis y reporte de seguridad que posteriormente permita identificar y notificar a la empresa en lo que se esté fallando.

Una conexión VPN es una forma segura de acceder de manera virtual a los recursos de una empresa desde cualquier parte del mundo, no obstante, se deben tener ciertas consideraciones

en el momento de importar el cliente mediante el cual se va a conectar el servidor, ya que si este archivo lo tienen personas que no están vinculadas con la empresa, se puede acceder fácilmente al servidor y robar información de este o alterar la información que contenga.

La seguridad informática debe ser utilizada tanto desde el ambiente local como desde el exterior, ya que muchas de las amenazas provienen desde el interior de las compañías, es por esto por lo que se hace indispensable que los usuarios que no cuentan con suficientes conocimientos en seguridad de redes informáticas no sean aislados del asunto, sino que por el contrario sean incluidos y capacitados.

Referencias bibliográficas

Bhargavan, K. y Leurent, G. (2016, octubre). On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN. En *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 456-467). ACM.

Diekmann, C., Michaelis, J., Haslbeck, M. y Carle, G. (2016, mayo). Verified iptables *firewall* analysis. En *2016 IFIP Networking Conference (IFIP Networking) and Workshops* (pp. 252-260). IEEE.

Dowd, P. W. y Mchenry, J. T. (2000). *U.S. Patent No. 6,141,755.* Washington, D. C.: U.S. Patent and Trademark Office.

Estados Unidos. (2018). *How to Protect Your Networks from Ransomware.* Recuperado de: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Foster, I., Kesselman, C. y Tuecke, S. (2001). The anatomy of the grid: Enabling scalable virtual organizations. *The International Journal of High Performance Computing Applications, 15*(3), 200-222.

Haralick, R. y Shapiro, L. (1991). Glossary of computer vision terms. *Pattern Recognition, 24*(1) doi: 10.1016/0031-3203(91)90117-N.

Hunt, R. (1998). Internet/Intranet *firewall* security—policy, architecture and transaction services. *Computer Communications, 21*(13), 1107-1123.

Liu, J., Li, Y., Van Vorst, N., Mann, S. y Hellman, K. (2009). A real-time network simulation infrastructure based on OpenVPN. *Journal of Systems and Software*, *82*(3), 473-485.

Lyu, M. R. y Lau, L. K. (2000). Firewall security: Policies, testing and performance evaluation. En *Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th Annual International* (pp. 116-121). IEEE.

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y. y Han, J. (2018). When intrusion detection meets blockchain technology: a review. *IEEE Access*, *6*, 10179-10188.

Naman Gupta, S. S. (2017). A *firewall* for internet of things. *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*, 2.

National Instruments. (2011). *FPGA Fundamentals*. Recuperado de: http://www.ni.com/white-paper/6984/es/#toc1

Panda Labs. (2017). *Informe trimestral Panda Labs, T2 2017.* Recuperado de: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/08/Pandalabs-2017-Q2-ES.pdf

Sánchez, J. A. M. (2004). Sistema de detección de intrusos en redes de comunicaciones utilizando redes neuronales.

Santiago, R. (2015). El modelo ADDIE y su relación con el diseño instruccional. *The Flipped Classroom*. Recuperado de: https://www.theflippedclassroom.es/el-modelo-addie/

Sharafaldin, I., Lashkari, A. H. y Ghorbani, A. A. (2018, enero). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. En *ICISSP* (pp. 108-116).

Sisterna, C. (s. f.). Field Programmable Gate Arrays (FPGAs). *Electrónica Digital II, Facultad de Ingeniería, Universidad Nacional de San Juan (Argentina).* Recuperado de: http://dea.unsj.edu.ar/sisdig2/Field%20Programmable%20Gate%20Arrays_A.pdf