Artículo original

Experiencia en la utilización de la Distribución GNU/Linux VyOS como software para PC-routers en una institución de Salud

Experience in the use of the GNU / Linux VyOS Distribution as software for PC-routers in a Health institution

Lic. Dayana Dagnesses Menés [1]

[1] Hospital Clínico Quirúrgico "Dr. Ambrosio Grillo Portuondo", Santiago de Cuba, Cuba

[*] Autora para la correspondencia: dayanadm@infomed.sld.cu

RESUMEN

En este trabajo se presenta una distribución de GNU/Linux que permite configurar un router, ***en un hardware x86*** de sobremesa, con casi todas las características de uno propietario; con el objetivo de mejorar la infraestructura de red, reducir costes, y aumentar la seguridad y disponibilidad de los servicios que se brindan; teniendo en cuenta además, las limitantes del país debido al bloqueo económico al cual está sometido por los Estados Unidos. Para ello se utilizó como método el análisis documental a partir de información recuperada en materiales digitales en Internet, así como experiencias realizadas en el Hospital Clínico Quirúrgico Universitario "Dr. Ambrosio Grillo Portuondo".

Palabras clave: enrutador; Cisco; Debian; VyOS; GNU/Linux; monitoreo de red

ABSTRACT

In this paper we present a GNU / Linux distribution that allows you to configure a router, in a desktop x86 hardware, with almost all the characteristics of a proprietary; with the aim of improving the network infrastructure, reducing costs, and increasing the security and availability of the services provided; also taking into account, the limitations of the country due to the economic blockade to which it is submitted by the United States. To do this, a documentary analysis was used as a method based on information retrieved from digital materials on the Internet, as well as experiences at the University Clinical Surgical Hospital "Dr. Ambrosio Grillo Portuondo ".

Palabras clave: router; Cisco; Debian; VyOS; GNU / Linux; network monitoring

Introducción

En la actualidad algunas de las tareas que deben realizar los administradores de redes son: gestionar la infraestructura de redes y comunicaciones, mantener la disponibilidad de los servicios existentes, proponer la inserción de nuevos dispositivos y servicios; previendo la evolución de su red según las necesidades de la organización y el alcance económico de la misma.

Cuba, un país bloqueado por Estados Unidos, se encuentra limitada en todo lo relacionado a lo económico y por tanto en la adquisición de tecnología adecuada para una infraestructura de última generación en todas sus empresas o instituciones. El Ministerio de Salud Pública no está exento de ello, la gran mayoría de las entidades carecen de este tipo de equipamiento prevaleciendo hardware obsoleto pero aún activo y del que se puede aprovechar su condición técnica con el software adecuado.

Las instituciones de salud de cada provincia se encuentran conectadas a través de ETECSA, empresa de telecomunicaciones que sirve de proveedor de Conectividad. Ésta, sitúa sus routers, los cuales están configurados con un direccionamiento IP y las tablas de rutas necesarias para su correcto funcionamiento en la red de salud INFOMED. No obstante, estos equipos no permiten ser gestionados ni administrados por ningún ente externo al proveedor del servicio; por lo que los administradores de red en salud se ven imposibilitados, entre otras cosas, de aplicar reglas de cortafuegos o listas de control de acceso para así cumplir con las políticas trazadas de seguridad informática.

Existen diferentes sistemas operativos software libre que pueden ser implementados sobre computadoras de sobremesa que sustituyen a los enrutadores capa 2 ó 3 con gran reconocimiento a nivel mundial; esto se debe a sus grandes costos. En determinadas infraestructuras de redes podemos encontrar uno o varios routers propietarios, pero en la mayoría de los casos prevalecen los routers Cisco [(1)], suministrados por **Cisco System**, uno de los principales proveedores de equipos de redes a empresas tecnológicas y otras organizaciones en

el mercado mundial. En la Figura 1 se muestra una tabla con las características de algunos enrutadores comerciales.

Router	Características	Ventaja	Transmisión	Precio
Cisco Gigabit Ethernet Router RV042G, Alámbrico, 6X RJ-45.	Tec. De cableado 10/100 base-T(X), conexión RJ-45. Protocolo de ruteo: IP, RIP-1, RIP-2.	Protocolos de red compactibles PPTP, L2TP, IPSec, PPPoE, DHCP.	Ethernet LAN, velocidad de transferencia de datos de 10/100/1000 Mbit/s.	$ 3,362
Cisco Megabit Router RV042G, Alámbrico, 6X RJ-45.	Tec. De cableado 10/100 base (T-X), conexión RJ-45. Protocolo de ruteo: IP, RIP-1, RIP-2.	Protocolos de gestión: SNMP, HTTP, HTTPS, Protocolos de red: PPTP, L2TP, IPsec, PPPoE y DHCP.	Ethernet LAN, velocidad de transferencia de datos de 10/100/1000 Mbit/s.	$ 3,414
Cisco Ethernet Router RV042, Dual WAN VPN, 10/100 4 Puertos.	Tec. De cableado 10/100 base-T(X), conexión WAN: RJ-45.	Protocolos de red compactibles: PPPoE, PPTP. Estándares de red: IEEE 802.3ab.	Ethernet LAN, velocidad de trasferencia de datos de 10, 100 Mbps/s.	$ 2, 731
Cisco Ethernet Router Multi-WAN RV016, 16x RJ-45.	Tec. De cableado: 10/100 base-T(x), Conexión WAN: Ethernet (RJ-45).	Protocolos de ruteo: RIP-1, RIP-2. Seguridad de Cortafuegos: SPI, DoS. Método de autenticación: MDS/SHAI.	Ethernet LAN, velocidad de trasferencia de datos: 10/100 Mbps/s.	$ 6, 818
Router D-LINK DIR 600	Provee entre dos a cuatro tiempos de tasa de transferencia de 11g, cuando se conecta a cliente 1x1 11n y Soporta función WMM para satisfacer los requerimientos de banda ancha de datos multimedia.	El router usa la tecnología Wireless 150, que ofrece mayor velocidad y rango que los estándares 802.11g/b. y una Configuración Protegida Wi-Fi (WPS).	Utiliza tecnología Wireless N, con una transferencia de 150 Mbps/s.	$ 350
Router D-LINK DIR810L	Crea una red que conecta todos los Computadores y Dispositivos móviles a su conexión de banda ancha a Internet a través de la nueva generación Wireless AC.	Permiten una conexión de alta velocidad por cable de hasta 4 PC u otros equipos. Permite navegar por la web, chatear y enviar correos electrónicos por la banda de 2,4 GHz.	Utiliza una tecnología Wireless AC750 Dual Band, con una transmisión de 750 Mbps.	$ 889
Router Smc Networks Barricade Inalámbrico	Gestión de red y soporte vpn, para una conexión inalámbrica de alta velocidad de hasta 54 mbps. Este router es multifuncional, de plataforma independiente, combina en un sólo dispositivo un switch de 4 puertos 10/100 mbps.	Contiene un Firewall spi (stateful packet inspection). Soporta vpn, Filtro de direcciones MAC y tiene Acceso protegido wi-fi (WPA).	Utiliza una tecnología wireless N, con una transmisión de 100 Mbps/s.	$ 399
Router WiFi N+ Dual Band PLAY N600 DBFUNCIÓN:	Ofrece la máxima velocidad de transferencia y minimiza los puntos muertos para que puedas disfrutar de un streaming de vídeo optimizado desde varios dispositivos en prácticamente cualquier punto de tu casa.	Conecta un disco duro externo para compartir fotos y archivos. Contiene estándares de cifrado WPS/WPA2 y seguridad preconfigurada, y utiliza Tecnología MultiBeam.	Este dispositivo utiliza una tecnología Wireless-N dual Band y ocupa una transmisión de 300 Mbps/s.	$ 934

Fig. 1- Tabla Comparativa de diferentes Modelos de Router

Se consideró oportuno la realización del presente trabajo con el objetivo de implementar un enrutador / cortafuegos basándose en una distribución GNU/Linux sobre un hardware de mediano rendimiento, atendiendo a las medidas y esquemas de seguridad establecidos en Cuba y cumpliendo con las normas internacionales de redes más actuales.

El objetivo general de este trabajo es describir y demostrar las posibilidades que brinda la distribución GNU/Linux en la implementación de routers de bajo costo en las infraestructuras de redes en instituciones de Salud. Para lograrlo fue preciso Identificar conceptos y definiciones utilizadas para este trabajo y desarrollar una metodología para la configuración e implementación del router con la distribución de GNU/Linux utilizada.

Esta investigación aporta la base necesaria para, primeramente, crear un diseño de infraestructura de red que logre un mejor aprovechamiento de los recursos disponibles; en segundo lugar, utilizar una herramienta que permita tener un mejor control de la seguridad de las redes, teniendo en cuenta la potencialidad que brinda GNU/Linux en este campo; y en tercer lugar, exponer una metodología para la implementación de un router estableciendo una serie de pasos para su correcta configuración en dependencia del entorno en el que se vaya a implementar.

Métodos

Conceptos, especificaciones y metodología de uso

Se realizó un análisis documental a partir de información recuperada en materiales digitales en Internet, así como experiencias realizadas en el Hospital Clínico Quirúrgico Universitario “Dr. Ambrosio Grillo Portuondo” y el intercambio conceptual con diferentes administradores de red en la provincia de Santiago de Cuba, relacionado con: enrutadores en GNU/Linux, router comercializables, herramientas de monitoreo de servicios de red, seguridad en redes, segmentación de red, entre otros. A partir de ello, se elaboró una propuesta de PC-router sobre una distribución GNU/Linux en la institución de salud Hospital Clínico Quirúrgico Universitario “Dr. Ambrosio Grillo Portuondo” que data de entre los años 2016 y 2018.

Los routers son unos de los elementos fundamentales de las redes actuales, los cuales permiten la interconexión entre ellas. En el caso de Cuba, la adquisición de determinados equipamientos tecnológicos de última generación se realiza a través de terceros países debido al bloqueo económico al que está sometido el país por parte del gobierno de los EE.UU. No obstante, existen soluciones libres que nos permiten tener un router en un hardware x86 utilizando herramientas basadas en GNU/Linux. Para el desarrollo de esta propuesta se escogió el VyOS [(2)].

Qué es VyOS?

A diferencia de OpenWRT o pfSense, VyOS es más similar a los routers tradicionales de hardware, focalizado en un buen soporte para características avanzadas de enrutamiento como protocolos de enrutamiento dinámico e interfaz de línea de comandos.

Ha sido un proyecto comunitario desde el principio. Cuando Vyatta Core fue interrumpido, un grupo de usuarios que querían seguir utilizándolo decidió usar la última versión disponible del código fuente para empezar con el proyecto **VyOS**, el cual se identifica con el logo que se muestra a continuación.

Fig. 2. Logo del proyecto VyOS.

VyOs, un sistema operativo enfocado a las funciones de red, proporciona capacidades de enrutamiento, cortafuegos y VPN. [(2)] Para hacer un símil es como disponer de un router Hewlett Packard o Cisco. Con una línea de comandos muy parecida a los dispositivos de red electrónicos y un consumo de recursos más ligero que los sistemas operativos completos.

Sus características incluyen la capacidad de ejecutarse tanto en plataformas físicas como virtuales. La interfaz de línea de comandos (CLI) es bastante clara, en ésta se puede importar, exportar y contiene todo para realizar routing tanto para protocolos IGP como EGP. Es una

distribución con muchas prestaciones, y al estar basada en Debian/Linux, es relativamente sencillo manejar los paquetes, actualizar, agregar, eliminar, etc.

En la figura se puede observar la interfaz de línea

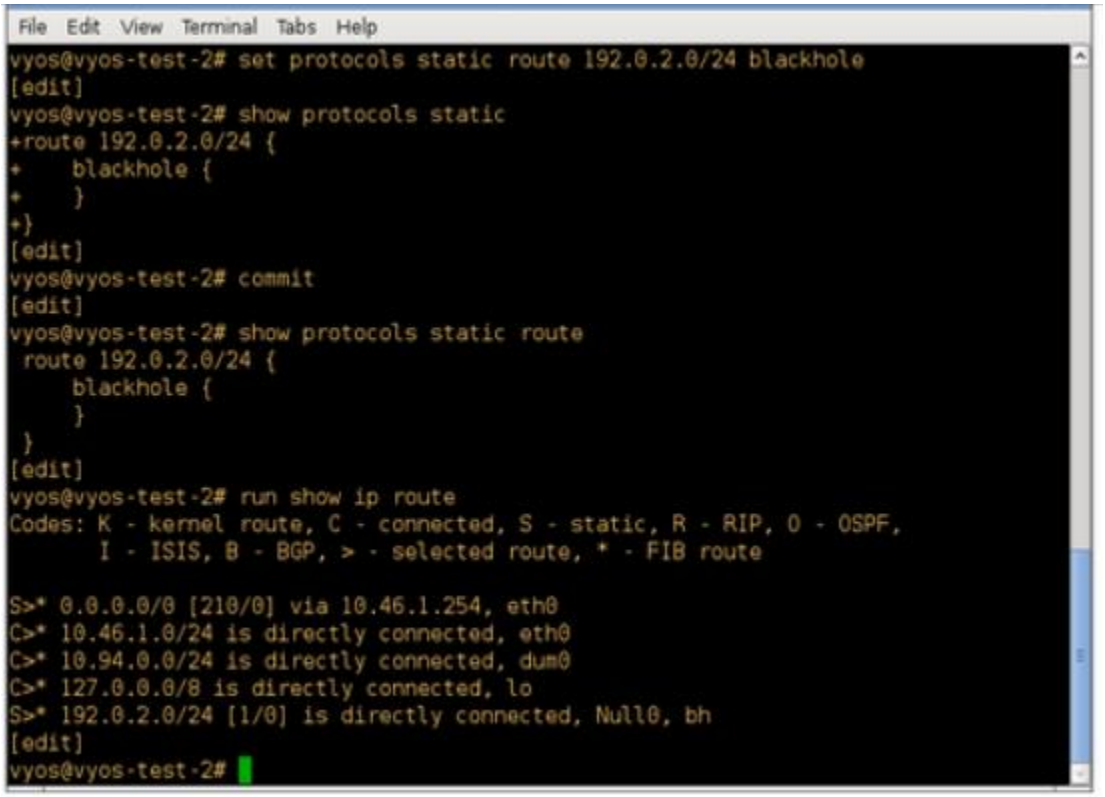

Fig. 3. Interfaz de línea de comando
Fuente: Vyos Project
http://vyos.net/wiki/Main_Page

Por qué utilizar VyOS?

Proporciona los siguientes servicios al más alto rendimiento:

- Enrutamiento avanzado: IPv4, IPv6, BGP, OSPF, RIP, VRRP, 802.1Q, etc.

- Segmentación de redes mediante VLAN.
- Seguridad: Cortafuegos, IPSec VPN, IDS, SSL VPN, Filtrado URL, etc.
- TUNNELING, VPN, NAT, DHCP, FLOW ACCOUNTING, PROXY
- Optimizador de rendimiento: QoS, Balanceador WAN, agrupación de enlaces, etc.
- Clusterización de alta disponibilidad e Integración con herramientas de monitoreo de redes.

Cómo utilizar VyOS?

En esta sección se describirán los recursos necesarios y la metodología que se empleó para poner a punto el PC-router en un período corto de tiempo.

Requerimientos técnicos

Los requerimientos mínimos para el PC-router son los siguientes:

- Microprocesador: Intel PIII 500 MHz CPU (mínimo recomendado) o superior.
- Memoria: 512 MB RAM (mínimo recomendado).
- Disco duro: 5 GB.
- Puertos: RS232 (para consola), y USB (arranque alternativo).

Un elemento que se tuvo en cuenta es el hardware de red a emplear. En este aspecto existen diversas opiniones, y basado en las consultas que se realizaron en muchos foros en Internet, las tarjetas de red con mejores prestaciones son las de marca Intel, dado que tienen un mejor comportamiento en infraestructuras de redes complejas donde la pérdida de paquetes debe ser la mínima posible; para el caso en que la topología de la red es sencilla, con una tarjeta de red Realtek basta. No obstante, ésta debe de tener las siguientes características principales:

- Velocidades de 100 Mbps, 1 Gbps, 10 Gbps.
- Soportar el estándar IEEE 802.1Q (VLAN tagging).
- Soportar el estándar IEEE 802.1P (Calidad de Servicio, QoS).
- Soportar el estándar IEEE 802.3X (Control de flujo Full Duplex).
- Soportar el estándar IEEE 802.3ad (Creación de agregación de enlaces, Bonding).

Teniendo en cuenta lo anterior, y la tecnología informática y de comunicaciones que es comercializada por empresas nacionales, las candidatas son las siguientes:

- Realtek RTL8139B, RTL8110SC (L), RTL8111C, RTL8169S. (PCI 32 y 64 bits).
- Allied Telesis (PCI 64 bits).
- Intel PRO/1000 GT/MT/PT de uno, dos o cuatro puertos, donde la GT es la más barata de todas. Estas tarjetas están recomendadas para redes donde se manejen muchas VLANs.

En este aspecto, es bueno aclarar que mientras se disponga de un Switch capa 2 completamente administrable, se logra implementar una topología de red que puede ser perfectamente escalable y modificable, dado que permiten la creación de LAN's virtuales o VLAN's para segmentar la red en diferentes subredes.

La conectividad entre el switch capa 2 y el PC-router sería a través de un puerto troncal. Ahora bien, en caso de no contar con un switch de estas características queda la opción de utilizar varias tarjetas de red en el PC-router.

Una vez escogido el hardware necesario se procede a instalar la distribución, la cual está situada en http://mirror.sliqua.com/vyos/.

Metodología de uso

A continuación se describe la metodología a seguir para implementar el PC-router [3,4,5]. Bajo ciertos entornos no será necesario ejecutar todos los pasos:

I. Instalación de la versión VyOS escogida.

II. Configuración de los adaptadores de red.

III. Habilitar SSH para el acceso remoto SSH.

IV. Configuración de las rutas necesarias (estáticas o dinámicas).

V. Configuración del protocolo NAT.

VI. Configuración de las reglas de cortafuegos necesarias: Existen dos formas de establecer las reglas. Una, es al estilo tradicional basado en la dirección del tráfico de

red que pasa por una interfaz de red determinada (IN/OUT), y la otra forma es mediante Políticas de Zona.

VII. Configuración y activación de los servicios de monitoreo de red (SNMP, NetFlow, etc.); los cuales serán la parte fundamental en la integración con herramientas de monitoreo externas como Cacti, Zabbix, ManageEngine NetFlow Analyzer y OSSIM.

VIII. Configuración de políticas de Calidad de Servicio (QoS) para servicios específicos que se deseen priorizar: Como ejemplos de ello tenemos el caso de los servicios de VoIP/TelefoníaIP y el caso de la transmisión de imágenes entre instituciones.

IX. Establecer los repositorios de actualizaciones y parches de seguridad.

Caso de uso y resultados

La infraestructura de red del hospital, así como los servicios que se ofrecen han ido en ascenso de manera gradual a partir del año 2012, sin embargo el enlace con el proveedor que es ETECSA cuenta con un único nivel de seguridad que es un servidor firewall Vyatta con dos interfaz de red.

La red LAN de la institución, a partir del año 2015 posee acceso pleno a internet y acceso a más de 200 cuentas de correos electrónicos con dominio institucional y alrededor de 150 en la red de salud INFOMED, todas con salida internacional. Así como 20 máquinas sin discos duros (o clientes ligeros) y áreas vulnerables como contabilidad y servidores de datos, mezcladas en un mismo segmento de red.

Demasiado tráfico en una sola subred, que presta varios servicios, limitándose el flujo de trabajo para las distintas áreas. Solucionar esto requiere pasar a niveles superiores en cuanto a la segmentación de la red.

Evaluando lo anteriormente descrito, y con la adquisición por parte de Brocade de Vyatta, y el abandono de la versión Community del popular router se procede a eliminarlo como PC-router y se instala el VyOS en su versión 1.1.7 en una computadora Pentium III con las siguientes características:

- CPU: Intel Pentium III 700 Mhz
- Memoria: 512 MB DIMMs
- HDD: Seagate IDE 40 GB
- Tarjeta de red: Modelo Realtek RTL8139C

Descripción de las subredes configuradas:

1. Red Externa INFOMED (eth0), aquí está el equipo directo a Internet, router del proveedor ETECSA (router Telindus 1421).
2. Subred local HGrillo (eth1), aquí estarán todas las computadoras del centro, excepto las descritas en los puntos 3 y 4.
3. Subred ContabHG (eth2), los host de Contabilidad.
4. Subred Servidores (eth3), servidores o máquinas como servidor.

Las interfaces 2, 3 y 4 están conectadas a puertos específicos de un switch TP-LINK SL2252WEB, el cual se configura atendiendo a su característica de soporte de VLAN's y direcciones MAC estáticas. En la siguiente figura se muestra la topología de red lógica de cómo quedó segmentada la red del hospital.

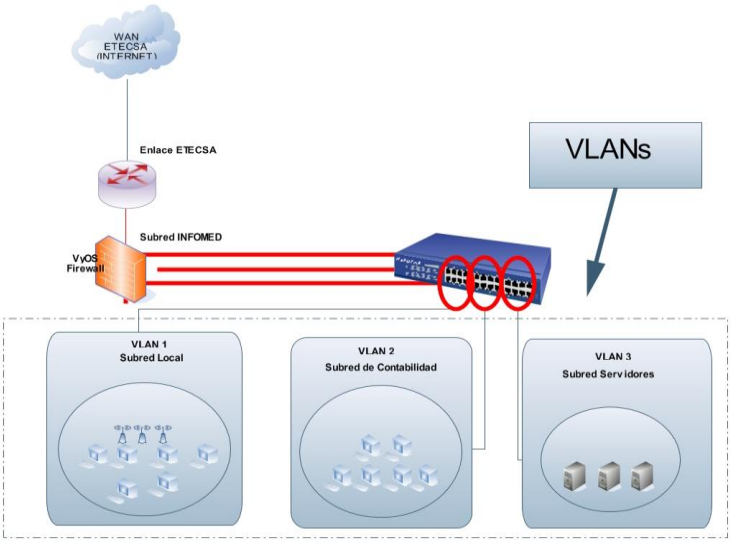

Fig. 4- Topología de la red Hospital Clínico Quirúrgico Universitario Dr. Ambrosio Grillo Portuondo.

Hasta este punto se han configurado los pasos del 1 al 5 de la metodología propuesta. Y se continúa estableciendo las reglas del cortafuego al estilo tradicional basado en la dirección del tráfico de red que pasa por una interfaz de red determinada (IN/OUT). Además, se activa el módulo de **SNMP y NetFlow** para monitorizar el comportamiento del mismo con herramientas externas que permitan monitorizar y visualizar gráficas y estadísticas de dispositivos conectados a una red.

Resultados

Se logra un mejor aprovechamiento del parque tecnológico de red con que cuenta la unidad permitiendo el diseño de una topología de red más eficiente y robusta.

- Se realiza la segmentación de la red interna teniendo en cuenta las 4 áreas más vulnerables de la institución en cuestión.
- Se logra la posibilidad del monitoreo de todo el tráfico de red.
- Se confirma que el software libre es más asequible para cualquier usuario, cumple con los estándares de calidad de servicio estando dentro de los rangos que permiten un buen desempeño de la conexión.

Conclusiones

- Brinda un cambio en cuanto a la forma de cómo las instituciones pueden mejorar su infraestructura de red utilizando tecnologías open source de la misma forma que si contaran con un modelo de red con equipamiento comercializable.
- Evidencia alta eficiencia y personalización en el manejo y monitorización de la infraestructura de red, según el entorno en que se utilice.

Referencias

1. CISCO [Internet]. California, USA: CISCO Systems. Soluciones de Seguridad de TI y redes de Cisco; [citado 20 Dic de 2016]; [aprox. 10 pantallas]. Disponible en: http://www.cisco.com/web/LA/soluciones/la/vpn/index.html.

2. Blog Josep Ma Solanes [Internet]. Español; c2013-2018. Router VyOS para laboratorios Hyper-V. [citado 20 Dic 2016]; [aprox. 65 pantallas]. Disponible en: https://www.jmsolanes.net/es/router-vyos-para-laboratorios-hyper-v/.

3. Top Computer Networking Guide [Internet]. How To Install and Configure Vyos Router-Basic Settings. [cited 2017 Feb 9]. Available from: https://topnetworkguide.com/how-to-install-and-configure-vyos-router/.

4. Vyos wiki [Internet]. Wiki; 2019 Jul. User Guide; [cited 2019 Dec]; [about 79 screens]. Available from: https://wiki.vyos.net/wiki/User_Guide.

5. Vyos User Guide [Internet]. International; c2019. Firewall; [updated 2019; cited 2019 Dec]. Available from: https://vyos.readthedocs.io/en/latest/firewall.html.

6. Ávila Gualdrón MA. Estudio de las mejores prácticas de ethical hacking, para generar un nuevo método que facilite la ejecución de análisis de seguridad enfocados a pruebas de penetración [monografía en internet]. Colombia: Universidad Nacional Abierta y a Distancia Escuela de Ciencias Básicas, Tecnología e Ingeniería Especialización en Seguridad Informática. 2018 [citado 14 Nov 2018]. 146 p. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/21293/4/1140816134.pdf.

7. Rivera Plata MA. Diseño de un modelo de infraestructura de interconexión para PYMES [tesis de grado ingeniería en sistemas internet]. Colombia: Universidad Libre, Facultad de Ingeniería. 2015 [citado 14 Nov 2018]. 49 p. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/8928/DOCUMENTO-TESIS%20FINAL%20ENTREGA%202%20DE%20AGOSTO.pdf?sequence=1&isAllowed=y.