05

Fecha de presentación: octubre, 2017
Fecha de aceptación: diciembre, 2017
Fecha de publicación: enero, 2018

PRÁCTICA

DE APLICACIÓN DE SEGURIDAD Y DISTRIBUCIÓN DE LAN CORPORATIVA

PRACTICE OF APPLICATION OF SECURITY AND DISTRIBUTION OF CORPORATE LAN

MSc. Jorge Humberto Tapia Celi[1]
E-mail: jorge.tapiac@ug.edu.ec
MSc. Alfonso A. Guijarro- Rodríguez[1]
E-mail: alfonso.guijarro@ug.edu.ec
MSc. Xavier Oswaldo Viteri Guevara[1]
E-mail: xavier.viterig@ug.edu.ec
[1] Universidad de Guayaquil. República del Ecuador.

Cita sugerida (APA, sexta edición)

Tapia Celi, J. H., Guijarro- Rodríguez, A. A., & Viteri Guevara, X. O. (2018). Práctica de aplicación de seguridad y distribución de LAN corporativa. *Universidad y Sociedad, 10(1)*, 41-45. Recuperado de http://rus.ucf.edu.cu/index.php/rus

RESUMEN

La alta demanda de en una red empresarial al área de TI nos incita a la incesante búsqueda de nuevas técnicas para precautelar y proteger la información generada por una empresa. Por esta razón, en este documento se diseñó una red LAN, en la cual aplicamos varias metodologías que permitió asegurar todos los componentes contra cualquier ataque, implementando VLANs, encriptación de contraseñas de acceso a switches, asignación de modos de accesos en los puertos del switch, cerrar interfaces no utilizadas y otros mecanismos determinantes que garantizan que los datos, objetos y recursos de una empresa no sean alterados; de tal modo, que permanezcan completos y que sean fiables. Aplicando estos métodos y técnicas convertimos a nuestra infraestructura de red en robusta, contra la detección y bloqueo de cualquier acceso no autorizado. Este diseño puede ser implementado en una PYME, garantizando el nivel de seguridad de la información y así mismo el cumplimiento de los estándares de seguridad requeridos hoy en el mercado.

Palabras clave: LAN, VLAN, switch, PYME, seguridad de la información, estándar de seguridad.

ABSTRACT

The high demand of security in the business network to the IT area incites us to the incessant search of new techniques to protect and protect the data of the company. The techniques learned in the subject of Computer Security are embodied in this article, which seeks to be a kind of manual to implement basic security in SMEs, addressing issues such as implementation of VLAN (VIRTUAL LOCAL AREA NETWORK), encryption of access passwords To switches, assigning access modes to switch ports, closing unused interfaces to improve our security level, and a number of techniques and methods to meet the security standards required today in the market.

Keywords: LAN, VLAN, switch, PYME, IT, informatic security, security standard.

INTRODUCCIÓN

Hoy en día todas las empresas consideran un factor importante implementar seguridad en sus comunicaciones, mediante este factor se intercambia información valiosa entre usuarios de la misma empresa, clientes y proveedores que mantienen el equilibrio del crecimiento del negocio.

Es por esto que las empresas, instituciones educativas, instituciones gubernamentales y demás entidades; a medida que se van creando y creciendo, parte de su activo principal es disponer de una adecuada infraestructura de red y una correcta distribución de sus intranets para asociar perfiles de usuarios a cada uno de ellas definiendo quienes tienen acceso a un determinado host; todo esto conlleva a que los hackers creen nuevas estrategias de ataque que hacen volver vulnerables nuestras redes, aprovechándose de aquellos negocios que no tienen un correcto diseño de redes, tampoco una implementación adecuada.

El objetivo de esta investigación es diseñar una distribución de una red LAN (Stallings, 2000). implementando seguridad de modo de acceso y administrativa para los componentes; logrando niveles de seguridad más altos para salvaguardar la integridad de información, creando perímetros de seguridad (Pérez Rivera, Britto Montoya & Isaza Echeverry, 2005), y así detectar y bloquear posibles ataques. Para esto se diseñó una red con capa core, capa de distribución y capa acceso. En esta última están creadas las VLANS (Stallings, 2000) (Redes Locales Virtuales) específicas que permitirán reducir el envío de tráfico de difusión y multicast a destinos no implicados. Además, usar mecanismos de seguridad como encriptación de claves de acceso, con el uso de algoritmos criptográficos (Forounzan, 2001), fiables en todos sus componentes entre ellos los switches, routers y otros que intervienen con el paso de los paquetes de datos.

Este documento está dividido en tres partes, la primera indica la introducción donde hacemos una revisión general sobre los parámetros importantes de la seguridad en las redes locales, en la segunda parte indicamos los métodos y materiales que utilizamos para implementar seguridad a la red; los cuales son experimentados en un simulador, en la tercera parte mostramos un análisis de los resultados, conclusiones y trabajos futuros sobra la investigación.

Debido al gran avance diario de la tecnología, y su naturaleza de las comunicaciones, cada vez es más difícil asegurar la información, de tal manera que su integridad esté garantizada; donde la responsabilidad de mantener a buen recaudo dicha data es el área de TI (Belloch, 2002).

Por tanto para armar nuestra red utilizaremos el software Cisco Packet Tracer el cual es un programa de simulación que permite experimentar con diseños de red y comprobar el comportamiento de las mismas (Cisco Systems, 2017). A continuación, indicaremos los componentes y la metodología con su respectiva configuración.

DESARROLLO

Los componentes a utilizar en Cisco Packet Tracer en su versión 7.0, se detallan en la tabla 1.

Tabla 1. Componentes utilizados.

Nº	Componentes
4	Switch Cisco 2960
7	PC's
1	Router CISCO 1841
2	Servidores

En la figura 1, visualizamos de manera completa la infraestructura de la red LAN.

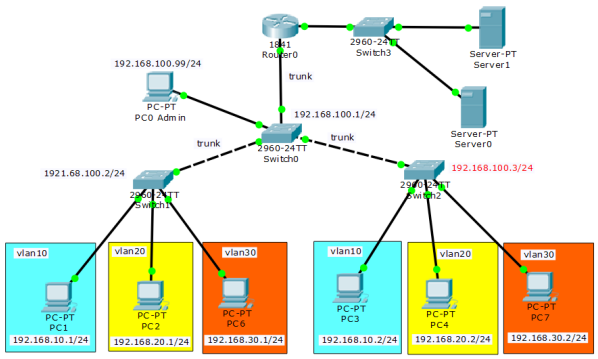

Figura 1. Diagrama de red.

En la tabla 2, se detallan las IP asignadas a cada componente y a que área pertenece cada una de ellas.

Tabla 2. Detalle de IP asignadas a componentes.

Componente	IP	Área
VLAN 10	192.168.10.0/24	Administración
VLAN 20	192.168.20.0/24	Sistemas
VLAN 30	192.168.30.0/24	Ventas
PC0	192.168.100.99/24	Admin - switch
VLAN 99	172.16.10.0/16	
Router	192.168.50.0/24	

A. Implementación de la configuración

Las configuraciones empleadas las detallaremos a continuación.

Direccionamiento lógico

Procedemos a asignar IP´s y su respectiva mascara de subred (Stallings, 2000) a los terminales dependiendo de la VLAN a la que vayan a ser asignados, donde la dirección IP va a ser la fuente de la información de los registros (Álvarez & Pérez, 2004); así mismo asignamos la dirección IP al router.

Seguridad en switches

Procedemos a incorporar seguridad en los switches por medio del CLI (Command Line Interface) con los siguientes comandos:

Switch(config)#line console 0

Switch(config-line)#password cisco

Switch(config-line)#login

Switch(config)#line vty 0 15

Switch(config-line)#password cisco

Switch(config)#service password-encryption

Switch(config)#enable secret cisco2

Hay que tomar en cuenta que las contraseñas usadas como cisco o cisco2, son de uso didáctico, de tal modo que se debe usar contraseñas más robustas y complejas, todo esto para que en caso de ser objeto de ataques, al atacante le tome mucho tiempo descifrar las contraseñas. Adicionalmente podemos incorporar otras medidas de seguridad como la incorporación de un banner para que pueda ser visualizarlo por todo aquel que desee ingresar a cualquiera de los switches.

Switch(config)#banner motd #ACCESO SOLO A PERSONAL AUTORIZADO#

```
ACCESO SOLO A PERSONAL AUTORIZADO
User Access Verification
Password:
```

Figura 2. Visualización de banner en el CLI

B. Creación de VLAN´s

Ya es hora de empezar a distribuir nuestra red corporativa en sus diferentes departamentos para eso haremos uso de las VLAN´s las cuales permiten la creación de subredes diferentes dentro de los equipos de comunicaciones como si de distintos elementos físicos se tratara, el tráfico no viaja cifrado, si no que es marcado con un identificador de la VLAN correspondiente, ocupándose el equipo de impedir la comunicación entre distintas redes según su configuración (Álvarez & Pérez, 2004).

Dependiendo de la interfaz que esté conectada cada PC, se asignó a cada interfaz de manera ordenada a cada VLAN y así mismo el modo de acceso de cada puerto.

- Empezaremos por crear la VLAN 99 la cual es para que acceda únicamente el administrador de los switches.

Switch(config)#VLAN 99

Switch(config-vlan)#name administracionsw

Switch(config-vlan)#exit

Switch(config)#interface vlan 99

Switch(config-if)#ip address 192.168.100.1 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

La dirección ip cambiara dependiendo del switch en el que estemos.

- Creación de VLAN para cada área de la empresa

Switch(config)#VLAN 10

Switch(config-vlan)#name administracion

Switch(config-vlan)#exit

Switch(config)#interface fastEthernet 0/0.10

Switch(config-if)#encapsulation dat1Q 10

Switch(config-if)#ip address 192.168.10.10 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

Y así seguimos asignando las VLAN de los siguientes departamentos en los switches.

Dependiendo de la interfaz asignamos el modo de acceso al puerto del switch.

Switch(config-if)#switchport mode access

Switch(config-if)#switch access vlan 10

Y en caso de que su uso sea de manera troncal asignamos el modo trunk; este enlace troncal es el que lleva la información de VLAN entre dispositivos de capa 2 preparados para la VLAN (IBM Knowledge Center, 2017).

Switch(config-if)#switchport mode trunk

- Cerrar interfaces no utilizadas en los switches

Para hacer más difícil el acceso a nuestra red y prevenir ataques procederemos a apagar interfaces que no estén en uso por el momento en la empresa, esta configuración la podemos realizar interfaz por interfaz o por rangos para reducer el tiempo de configuración.

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#shutdown

La siguiente forma es por rangos, para hacerlo de forma rápida, previo a cada cierre de interfaces, se debe consultar las interfaces no utilizadas, de lo contrario perjudicamos el desarrollo de las actividades de la empresa.

Switch(config)#interface range fastEthernet 0/5-16

Switch(config-if-range)#sh

Switch(config-if-range)#shutdown

- Configuración de servidores

Se procedió a configurar dos servidores; solo en uno se configuro el servidor de correo, pero en ambos servidores se configuró el DNS (Domain Name System), que es un conjunto de protocolos y servicios que va a permitir a los usuarios utilizar los nombres en vez de tener que recordar la direcciones IP.

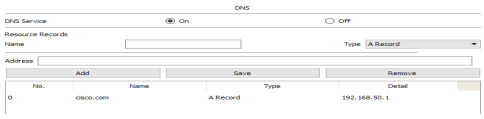

Figura 3. Configuración usada en el servidor DNS

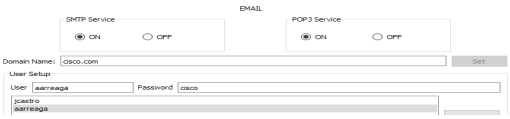

Figura 4. Configuración usada en el servidor EMAIL

C. Seguridad Triple AAA con Base de Datos Radius

Este tipo de seguridad es quién permite controlar el acceso a una red (autentificación) y qué puede hacer el usuario mientras este allí (autorización), así como auditar que acciones realizan al acceder a la red(registro de auditoría) (Andreu Mediero, 2014). A continuación mostramos de qué manera se configura ese tipo de seguridad.

Router>enable

Router#configure terminal

Router(config)#aaa new-model

Router (config)#username andres secret Jimenez1995

Router(config)#aaa authentication login default local

Router(config)#radius-server host 192.168.50.1

Router(config)#radius-server key Jimenez1995

Router(config)#aaa authentication enable default group radius enable

Router(config)#^Z

D. Hardening

Las operaciones seguras en la red es un tema sustancial, donde se debe crear avisos y respuestas de seguridad, para ello se han determinado las siguientes vulnerabilidades que pueden constituir una amenaza contra nuestra red, para luego convertirlas en bloqueo de posibles ataques.

- Desactivar servicios a las interfaces.
- Router(config-if)#no ip proxy-arp
- Deshabilitar puertos no utilizados.

line console 0

no exec

line aux 0

no exec

- Bloqueo de ataques de fuerza bruta: Este ataque se caracteriza en el cual se controla el número de intentos exitosos y fallidos en el router. Cada vez que se incrementa el abecedario y/o la longuitud de la cadena, la cantidad de combinaciones que puede llegar a surgir crece estrepitosamente (López, 2013).

Router#configure terminal

Router(config)#login block-for 60 attempts 3 within 50

Aquí le indicamos que bloquee un número de segundos el acceso por ssh, telnet y http cuando se realizaron n intentos fallidos en un intervalo de segundos determinado.

Registro de los intentos fallidos a partir de un número.

Router(config)#login on-failure log

Registro de accesos exitosos

Router(config)#login on-success log

- Asegurar los archivos (IOS y archivo de configuración)

La **resilient configuration** permite proteger la IOS y el archivo de configuración de borrados accidentales o modificaciones fraudulentas de por ejemplo un hacker habilidoso.

Router#configure terminal

Router(config)#secure boot-image

Router(config)#secure boot-config

CONCLUSIONES

El diseño de redes locales e implementación, es una tarea bastante amplia; por tanto, hemos logrado configurar una red local aplicando niveles de seguridad aceptados en el entorno local que permitió que nuestra red sea robusta y fiable. Es importante reconocer la asignación de

las respectivas terminales a sus respectivas áreas como se puede observar en la Figura 1 no se encuentran físicamente en el mismo switch, de tal manera, hemos conseguido que a pesar de estar distantes pueden seguir laborando en su área específica, todo esto creando VLANs y poniendo en modo de acceso distintos en las respectivas interfaces de switches.

Como punto adicional, es recomendable que el lector considere que la seguridad de todo dispositivo depende de quien lo administre, para esto se recomienda el uso adecuado de contraseñas y la encriptación de las mismas con algoritmos complejos, como en este caso utilizamos el cifrado tipo 7 de cisco y md5.

Este prototipo que hemos desarrollado en este artículo está diseñado de manera escalable, para que así en un trabajo futuro se pueda implementar en una empresa y a esto agregar un gestor unificado de amenazas para un mejor control de acceso y otros componentes que sirvan de complemento para garantizar la integridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, G., & Pérez, P. P. (2004). ***Seguridad informática pra empresas y particulares***. Madrid: Mc Graw Hill.

Andreu Mediero. E. (2014). ***Seguridad Informática y Alta disponibilidad***. San Francisco: Scribd Inc. Recuperado de https://www.scribd.com/document/324602057/Seguridad-Informatica-y-Alta-Disponibili-pdf

Belloch, C., Mide, D., & De Valencia, U. (2002). Las Tecnologías de la Información y Comunicación en el aprendizaje. Valencia: Universidad de Valencia. Recuperado de http://www.uv.es/bellochc/pedagogia/EVA1.pdf

Cisco Systems. (2017). Cisco Packet Tracer. San José: Cisco Systems.

Forounzan, B. A. (2001). ***Transmisión de Datos y redes de comunicaciones***. Madrid: Mc Graw Hill.Molina Ruiz, J. E. (2012). Propuesta de segmentación con redes cirtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en Empresa Editora el Comercio Planta Norte. Tesis de pregrado. Chiclayo: Universidad Católica Santo Toribio de ***Mogrovejo.*** Recuperado de http://tesis.usat.edu.pe/handle/usat/522?locale=es

IBM Knowledge Center. (2017). ***Enlace troncales***. Las Vegas: IBM Knowledge Center. Recuperado de https://www.ibm.com/support/knowledgecenter/es/SS-2GNX_7.1.1/com.ibm.tivoli.tpm.scenario.doc/network/cnet_trunking.html

López, V. (2013). Papel de la explosión combinacional en ataques de fuerza bruta. Investig.innov.ing., ***1(1),*** 28-32. Recuperado de http://revistas.unisimon.edu.co/index.php/innovacioning/article/view/2069/2907

Pérez Rivera, C. A., Britto Montoya, J. A., & Isaza Echeverry, G. A. (2005). Aplicación de redes neuronales para la detección ded intrusos en redes y sistemasa de información. Scientia ***et*** Technica, 11(27). Recuperado de http://www.redalyc.org/html/849/84911698042/index.html

Stallings, S. (2000). ***Comunicaciones y redes de computadores.*** México: Prentice Hall.