**Instituto Tecnológico de Mexicali**

**Practica 2.2.4.11**

**Carrera:**

Ingeniería en Sistemas Computacionales

**Nombre del Alumno(a):**

Martínez Yebra Beatriz Andrea

#13490929

**Nombre del profesor(a):**

MC Heber Samuel H. Tabares

**Materia:**

Administración de Redes de Computadoras

**Horario:**

12:00 p.m. – 1:00 p.m.

Mexicali Baja California, Jueves 14 de Septiembre 2017.

**Configuración de características de seguridad de switch**

**Paso 3. Configurar los parámetros básicos en S1.**

Una buena práctica de seguridad es asignar la dirección IP de administración del switch a una VLAN distinta de la VLAN 1. En este paso, se creará la VLAN 99 en el switch y le asignará una dirección IP.

1. Configure el nombre del dispositivo.
2. Desactive la búsqueda del DNS.
3. Asigne class como la contraseña del modo EXEC privilegiado.
4. Asigne cisco como la contraseña de vty y la contraseña de consola, y luego habilite el inicio de sesión.
5. Configure un Gateway predeterminado para el S1 con la dirección IP del R1.
6. Cifre las contraseñas de texto no cifrado.
7. Guarde la configuración en ejecución en la configuración de inicio.
8. Cree la VLAN 99 en el switch y asígnele el nombre **Management.**

S1(config)# vlan 99

S1(config-vlan)# name **Management**

S1(config-vlan)# exit

S1(config)#

1. Configure la dirección IP de la interfaz de administración VLAN 99, tal como se muestra en la tabla de direccionamiento, y habilite la interfaz.

S1(config)# interface vlan 99

S1(config-if)# ip address 172.16.99.11 255.255.255.0

S1(config-if)# no shutdown

S1(config-if)# end

S1#

1. Emita el comando **show vlan** en el S1. **¿Cuál es el estado de la VLAN 99?** Active
2. Emita el comando **show ip interface brief** en el S1. **¿Cuál es el estado y el protocolo para la interfaz de administración VLAN 99?** El estado es up y el protocolo figura como down.

**¿Por qué el protocolo figuro como down, a pesar de que se emitió el comando no showutdown para la interfaz VLAN 99?** No se asignaron puertos físicos en el switch a la VLAN 99.

1. Asigne los puertos F05/ y F0/6 a la VLAN 99 en el switch.

S1# config t

S1(config)# iterface f0/5

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 99

S1(config-if)# interface f0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 99

S1(config-if)# end

1. Emita el comando **show ip interface brief** en el S1. **¿Cuál es el estado y el protocolo que se muestra para la interfaz VLAN 99?** Up – Up

**Paso 4. Verificar la conectividad entre los dispositivos.**

1. En la PC-A, haga ping a la dirección de Gateway predeterminado en el R1. **¿Los pings se realizaron correctamente?** Si
2. En la PC-A, haga ping a la dirección de administración del S1. **¿Los pings se realizaron correctamente?** Si
3. En el S1, haga ping a la dirección de Gateway predeterminado en el R1. **¿Los pings se realizaron correctamente?** Si
4. En la PC-A, abra un navegador web acceda a <http://172.16.99.11>. Si le solicita un nombre de usuario y una contraseña, deje el nombre de usuario en blanco y utilice la contraseña class. Se le solicita una conexión segura, conteste No. **¿Pudo acceder a la interfaz web en el S1?** Si
5. Cierre la sección del explorador en la PC-A.

**Parte 3. Configurar y Verificar el acceso por SSH en el S1.**

* **¿Qué versión de SHH usa el switch?** 1.99
* **¿Cuántos intentos de autenticación permite SSH?** 3
* **¿Cuál es la configuración predeterminada de tiempo de espera para SHH?** 120 segundos

**Paso 2. Modificar la configuración de SHH en el S1.**

* **¿Cuántos intentos de autenticación permite SSH?** 2
* **¿Cuál es la configuración de tiempo de espera para SSH?** 75 segundos

**Paso 3. Verificar la configuración de SSH en el S1.**

* **¿La conexión se realizó correctamente?** Si
* **¿Qué petición de entrada se mostró en el S1?, ¿Por qué?** El S1 muestra la petición de entrada en el modo EXEC privilegiado porque la opción privilegie 15 segundo de usó al configurar el nombre de usuario y la contraseña.

**Parte 4. Configurar y Verificar las características de seguridad en el S1**

**Paso 1. Configurar las características de seguridad general en el S1.**

1. Configure un aviso de mensaje del día (MOTD) en el S1 con un mensaje de advertencia de seguridad adecuado.
2. Emita un comando **show ip interface brief** en el S1. **¿Qué puertos físicos están activos?**

Los puertos f05/ y F0/6

1. Desactive todos los puertos sin utilizar en el switch. Use el comando **interface range**.

S1(config)# interface range f0/1 – 4

S1(config-ip-range)# shutdon

S1(config-ip-range)# interface range f0/7 – 24

S1(config-ip-range)# shoutdown

S1(config-ip-range)# end

S1#

1. Emita el comando show ip interface brief en el S1. **¿Cuál es el estado de los puertos F0/1 a F0/4?** Administratively down.
2. Emita el comando show ip http server status.

**¿Cuál es el estado del servidor HTTP?** Enabled

**¿Qué puerto del servidor utiliza?** 80

**¿Cuál es el estado del servidor seguro de HTTP?** Enabled

**¿Qué puerto del servidor seguro utiliza?** 443

1. Las sesiones HTTP envían todo como texto no cifrado. Deshabilite el servicio HTTP que se ejecuta en el S1.

S1(config)# no ip http server

1. En la PC-A, abra una sesión de navegador web a <http://172.16.99.1>. **¿Cuál fue el resultado?**

No se puede abrir la página web. El S1 rechaza las conexiones HTTP.

1. En la PC-A, abra una sesión segura de navegador web en <https://172.16.99.11>. Acepte el certificado. Inicie sesión sin nombre de usuario y con la contraseña class. **¿Cuál fue el resultado?** La sesión web segura se inició correctamente.

**Paso 2. Configurar y Verificar la seguridad de puertos en el S1.**

1. Registe la dirección MAC de G0/1 del R1. Desde la CLI del R1, use el comando show interface g0/1 y registre la dirección MAC de la interfaz.

R1# show interface g0/1

GigabitEthernet0/1 is up, line protocol is up

Harware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 3047.0da3.1821)

**¿Cuál es la dirección MAC de interfaz G0/1 del R1?** 30f7.0da3.1821

1. Desde la CLI de S1, emita un comando show mac address-table en el modo EXEC privilegiado. Busque las entradas dinámicas de los puertos F0/5 y F0/6. Regístrelos a continuación.

Dirección MAC de F0/5: 30f7.0da3.1821

Dirección MAC de F076: 00e0.b857.1ccd

1. Configure la seguridad básica de los puertos.
2. Desde la CLI del S1, ingrese al modo de configuración de interfaz para el puerto que se conecta al R1.

S1(config)# interface f0/5

1. Desactive el puerto.

S1(config-if)# showdown

1. Habilite la seguridad de puertos en F0/5.

S1(config-if)# switchport port-security

1. Configure una entrada estatica para la dirección MAC de la interfaz G0/1 del R1 registrada en el paso 2a.

S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx

(xxxx.xxxx.xxxx es la dirección MAC de la interfaz G0/1 dek router)

1. Habilite el puerto del switch.

S1(config-if)#no shotdown

S1(config-if)# end

1. Verifique la seguridad de puertos en F0/5 del S1 mediante la emisión de un comando show port-security interface.

**¿Cuál es el estado del puerto de F0/5?** Secure-up, que indica que el puerto es seguro, pero el valor del estado y el protocolo es up.

1. En el modo EXEC privilegiado del R1, haga ping a la PC-A. **¿El ping se realizó correctamente?, ¿Por qué o Por qué no?** No, el puerto F0/5 en el S1 está desactivado debido a la violación de seguridad.

**REFLEXIÓN**

1. **¿Por qué habilitaría la seguridad de puertos en un switch?**

Ayudaría a evitar que los dispositivos no autorizados accedan a su red en caso de que se conectaran a un switch en su red.

1. **¿Por qué deben deshabilitarse los puertos no utilizados en un switch?**

Una excelente razón es que un usuario no podría conectar un dispositivo al switch en un puerto sin utilizar para acceder a la LAN.