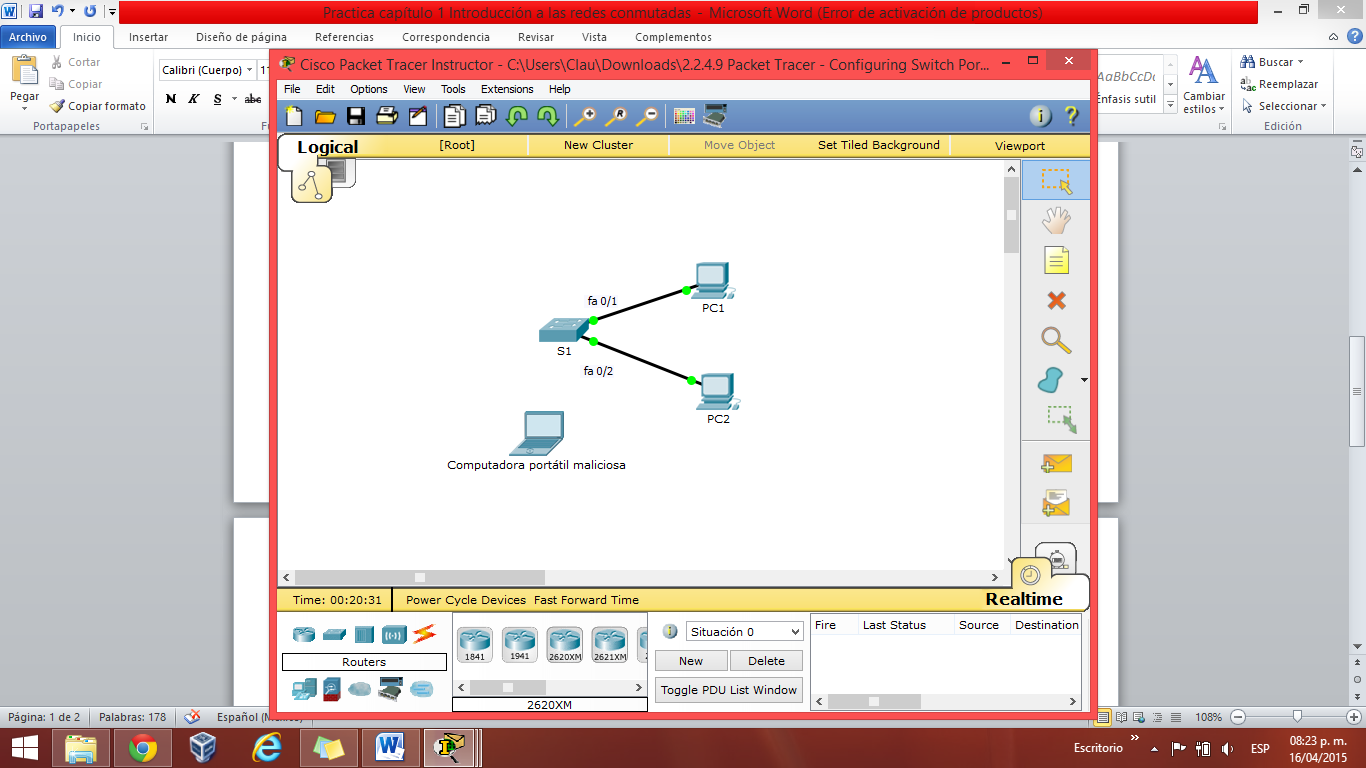
**Objetivo:**

Configurar SSH y seguridad en los puertos del Switch

**Topología:**

Realiza el cableado físico de la siguiente topología.



**Tabla de direccionamiento:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dispositivo** | **Interfaz** | **Dirección ip** | **Mascara de subred** |
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |
| Computadora portátil maliciosa | NIC | 10.10.10.12 | 255.255.255.0 |

**Instrucciones:**

**Configuración básica del switch**

* Configura un nombre al switch, hostname:S1

**S1 (config)#hostname S1**

* Configura contraseña en el switch para acceso a modo privilegiado

**S1 (config)#enable password universidad**

**O**

**S1 (config)#enable secret universidad**

* Configura una contraseña para acceso a la consola

**S1 (config)#line console 0**

**S1 (config-line)#password cisco**

**S1 (config-line)#login**

**Configuración de SSH para acceso remoto**

* Crea la interfaz virtual 1 y asígnale la dirección ip correspondiente según la tabla de direccionamiento.

**S1 (config)#interface vlan 1**

**S1 (config-if)#ip address x.x.x.x x.x.x.x**

**S1 (config-if)#no shutdown**

* Configura el nombre de dominio cisco.com

**S1 (config)#ip domain-name cisco.com**

* Genera las claves RSA con longitud 1024

**S1 (config)#crypto key generate rsa**

The name for the keys will be: S1.S1

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: **1024**

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

* Crea al usuario: administrador, contraseña: redes

**S1 (config)#username administrador password redes**

* Configura las líneas VTY para permitir SSH para acceso remoto

**S1 (config)#line vty 0 15**

**S1 (config-line)#transport input ssh**

**S1 (config-line)#login local**

**Pruebas para acceso remoto:**

* Realiza la conexión remota al switch vía SSH desde la PC1.

Desde símbolo del sistema:

**PC> ssh -l administrador 10.10.10.2**

**Open**

**Password:**

**s1> enable**

* Cierra la conexión y ahora hazla desde la PC2

**Configuración de Seguridad en los puertos del switch**

* Configura el puerto fa 0/1 y 0/2 como modo acceso para quitar la configuración por default de modo dynamic de los puertos y enseguida habilita seguridad en el rango de puertos fastEthernet 0/1-2

**S1 (config)#interface range fastEthernet 0/1-2**

**S1 (config-if-range)#switchport mode access**

**S1 (config-if-range)#switchport port-security**

* Configura la seguridad máxima en ambos puertos de tal forma que solo un dispositivo pueda acceder a los puertos con seguridad.

**S1 (config-if-range)#switchport port-security máximum 1**

* Configura la infracción en ambos puertos, de tal forma de que si se produce una violación se deshabiliten.

**S1 (config-if-range)#switchport port-security violation shutdown**

**S1 (config-if-range)#exit**

* Habilita el aprendizaje de MAC en la fa 0/1 de forma dinámica y que se agregue a la configuración en ejecución.

**S1 (config)#interface fastEthernet 0/1**

**S1 (config-if)#switchport port-security mac-address sticky**

**S1 (config-if)#exit**

* Habilita el aprendizaje de MAC en la fa 0/2 de forma estática.

**S1 (config)#interface fastEthernet 0/2**

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

**S1 (config-if)#exit**

* Desactiva los puertos que no están habilitados con seguridad.

**S1 (config)#interface range fastEthernet 0/3-24**

**S1 (config-if-range)#shutdown**

**S1 (config)#interface range gigabitEthernet 0/1-2**

**S1 (config-if-range)#shutdown**

**S1 (config-if-range)#exit**

**Pruebas para seguridad en los puertos:**

* Verifica que efectivamente este habilitada la seguridad en los puertos correspondientes y que el aprendizaje único de MAC coincida con la dirección MAC de la PC1 en la fa 0/1 y la dirección MAC de la PC2 en la fa 0/2.

**S1#show port-security interface fastEthernet 0/1**

Port Security : **Enabled**

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : **00D0.D3B1.695E:1**

Security Violation Count : 0

* Desconecta la PC1 y conecta la pc portátil maliciosa ya sea a la fa0/1 o fa 0/2, intenta hacer ping a la interfaz virtual del switch (10.10.10.2) o hacer una conexión de acceso remoto vía ssh, observa que sucede con la interfaz.

¿Cuál es la razón de lo ocurrido?

¿Cuál sería el resultado si el aprendizaje máximo de MAC por puerto fuera 2?

* Vuelve a conectar la PC1 a la fa 0/1.

¿Cuál es el status de la interfaz?, ¿Qué tienes que hacer para solucionarlo?

Para volver a restablecer la interfaz después de haberle sido aplicada la restricción shutdown, entra a la interfaz y primero aplica el comando de deshabilitacion y enseguida el de habilitación de interfaz.

**S1(config)#interfaz fastEthernet 0/1**

**S1(config-if)#shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

**S1(config-if)#no shutdown**

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Observaras que la interfaz es restablecida.