Desafío - Controles de seguridad

En este desafío validaremos nuestros conocimientos de configuración de una red de datos y la implementación de listas de acceso en capas . Para lograrlo, necesitarás aplicar el archivo M5_U1_Desafio.pkt.

Lee todo el documento antes de comenzar el desarrollo **individual** para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

// Tiempo asociado: 1 hora cronológica.

Descripción

Una empresa requiera implementar una pequeña red corporativas con soluciones de VLANs, puertos de acceso, enlaces troncales, enrutamiento intervlan, enrutamiento dinámico y estático. Luego de eso implementar listas de acceso que operen en capa 3 y capa 4 para controlar el tráfico en ciertos escenarios requeridos.

Aplicando los conceptos y herramientas aprendidas hasta ahora, tendrás que realizar este desafío.

Conocimientos requeridos para el desafío:

¿Qué es Port Security?

Port Security es una función de seguridad en switches que restringe el acceso a un puerto físico en función de las direcciones MAC permitidas.

Objetivo: Evitar que un usuario no autorizado (por ejemplo, alguien que conecta su laptop en un puerto del switch) acceda a la red.

¿Para qué se emplea?

Evitar suplantación de dispositivos (MAC spoofing).
Controlar cuántos dispositivos pueden conectarse por puerto.
Mejorar la seguridad en entornos físicos (oficinas, laboratorios, aulas).
Aplicar medidas de bloqueo o alerta cuando se detecte algo no autorizado.

Paso a paso: Implementación en Packet Tracer
Escenario:
Tienes un Switch (Switch0) y dos PCs: PC1 (permitido) y PC2 (no autorizado). Se conectan al puerto FastEthernet 0/1 del switch.

Comandos con explicación línea por línea:

Switch> enable
Switch# configure terminal

Entras al modo privilegiado y luego a configuración global.

Switch(config)# interface fastEthernet 0/1

Accedes al puerto donde está conectado el dispositivo autorizado (PC1).

Switch(config-if)# switchport mode access

Pones el puerto en modo "acceso", es decir, no es troncal, solo pertenece a una VLAN.

Switch(config-if)# switchport port-security

Activamos la seguridad de puerto en ese puerto. Este comando por sí solo no hace nada aún, pero habilita el modo.

Switch(config-if)# switchport port-security maximum 1

Establece un máximo de 1 dirección MAC válida por puerto (solo 1 dispositivo permitido).

Switch(config-if)# switchport port-security violation restrict

Indica que si se conecta un dispositivo no autorizado, el switch va a restringir el tráfico de ese dispositivo y registrar el intento (log).

Otras opciones son:

protect: descarta el tráfico pero no genera alerta.
shutdown: desactiva el puerto completamente si detecta una MAC no autorizada.

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

Permite que el switch aprenda automáticamente la MAC del primer dispositivo conectado, y la guarde como permitida.
(Opcionalmente, puedes configurarla de forma manual).

Switch(config-if)# end
Switch# write memory

Sales de la configuración y guardas los cambios en la memoria para que no se pierdan al reiniciar.

¿Qué es DHCP?

DHCP (Dynamic Host Configuration Protocol) permite que los dispositivos obtengan automáticamente una dirección IP, máscara, gateway, DNS, etc., desde un servidor DHCP, evitando configuraciones manuales.

Comandos de configuración en el router explicados:

```
Router> enable
Router# configure terminal

! Activar interfaz que conecta al switch
Router(config)# interface g0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown

! Crear pool DHCP
Router(config)# ip dhcp pool LAN
Router(dhcp-config)# network 192.168.1.0 255.255.255.0   ! Red objetivo
Router(dhcp-config)# default-router 192.168.1.1          ! Gateway
Router(dhcp-config)# dns-server 8.8.8.8                  ! DNS opcional

! Excluir direcciones que no deben asignarse por DHCP
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.99
```

Comandos de configuración en un router con VLANS (Sub Interfaces)

```
Router> enable
Router# configure terminal

! Subinterfaz para VLAN 10
Router(config)# interface g0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0

! Subinterfaz para VLAN 20
Router(config)# interface g0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0

! Activar interfaz física
Router(config)# interface g0/0
```

```
Router(config-if)# no shutdown

! Configurar pool DHCP para cada VLAN
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1

Router(config)# ip dhcp pool VLAN20
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1

! Excluir direcciones reservadas en cada VLAN
Router(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
Router(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.9
```

Requerimientos

1. Implementar VLANs, Puertos de Acceso y Troncales según requerimientos solicitados. (**2 Puntos**)

2. Implementar Enrutamiento Intervlan, DHCP según requerimientos solicitados. (**2 Puntos**)

3. Implementar protocolos de enrutamiento dinámico y estático según requerimientos solicitados. (**2 Puntos**)

4. Implementar listas de control de acceso según los requerimientos solicitados. (**2 Puntos**)

5. Comprobar el funcionamiento de las listas de control de acceso según requerimientos solicitados. (**2 Puntos**)

 ¡Mucho éxito!

Consideraciones y recomendaciones