**Ejercicio 2- Seguridad en capa 2: Seguridad en los puertos de acceso de conmutadores LAN**

En la red de la compañía XYZ, recientemente, se han producido varios ataques originados desde el interior de la propia red. Por esta razón, la dirección ha solicitado al responsable de la red mejorar el control de acceso a la LAN. Para evitar los ataques de desbordamiento de la tabla de MACs de los conmutadores, el responsable ha decidido configurar la seguridad por puerto y, de esta manera, poder limitar el número de direcciones MAC que por puerto cada conmutador aprenda. Si el número de direcciones MAC excede el límite establecido, se establece que el puerto quede fuera de servicio de manera automática. Por otro lado, el administrador también pretende controlar el acceso a la red LAN a través de la MAC de los equipos de usuario. En este ejercicio se practica con las funcionalidades que, para conseguir todo lo anterior, incorporan los equipos de CISCO Systems.

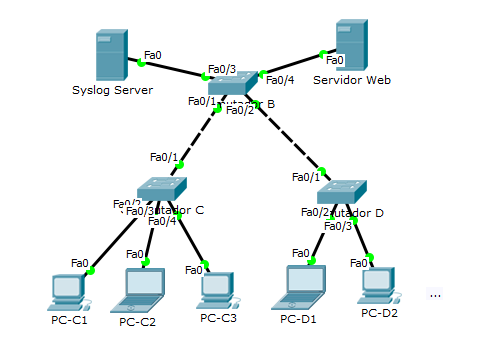


Figura 1. Topología de la red de la empresa XYZ

**Guion de la práctica**

**Tarea 1:** Construir la red de la figura 1. Para la asignación de direcciones IP a los equipos utilizar la red 10.1.1.0/24. Rellenar la tabla siguiente con las asignaciones de las direcciones ip.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | **Dirección ip/máscara de red** | **Dirección física** | **Conmutador/Interfaz (inicial)** |
| Conmutador D | 10.1.1.70 / 255.255.255.0 |  |  |
| Conmutador C | 10.1.1.60 / 255.255.255.0 |  |  |
| Conmutador B | - | - | - |
| - |
| Servidor Web | 10.1.1.1 / 255.255.255.0 | 0006.2AC8.8CC2 | FastEthernet0 |
| Syslog Server | 10.1.1.50 / 255.255.255.0 | 00D0.D3A9.398A | FastEthernet0 |
| PC-C1 | 10.1.1.2 / 255.255.255.0 | 00E0.F99D.E464 | FastEthernet0 |
| PC-C2 | 10.1.1.3 / 255.255.255.0 | 00E0.8F44.7ED5 | FastEthernet0 |
| PC-D1 | 10.1.1.4 / 255.255.255.0 | 0001.C7D1.C962 | FastEthernet0 |
| PC-D2 | 10.1.1.5 / 255.255.255.0 | 00E0.B088.8AC5 | FastEthernet0 |

**Tarea 2:** Una vez creada la red en CPT y asignadas las direcciones ip, pasar a realizar la configuración de red básica únicamente de los sistemas finales. Una vez realizada esta configuración, comprobar que existe conectividad entre todos estos sistemas.

**Tarea 3:** Configuración Syslog para registrar las incidencias que se produzcan

* Paso 3.1: Configurar el servicio de syslog en “Servidor Syslog”. Para ello, realizar los pasos siguientes:

Seleccionar “Servidor Syslog” 🡪 Pestaña *Services* 🡪 *S*eleccionar Syslog del listado de SERVICES 🡪 seleccionar ON en caso que esté en OFF

* Paso 3.2: Configurar los conmutadores de acceso para que envíen los mensajes al Servidor Syslog:
  + Configurar el conmutador C para estampar el tiempo en los mensajes. Proceder de la siguiente forma:

SWC(config)# service timestamps log datetime msec

* + Configurar conmutador C para enviar los mensajes al servidor syslog

SWC(config)# logging host 10.1.1.50 (dirección IP ejemplo, utilizar la correspondiente)

* + Configurar dirección ip en conmutador C

SWC(config)# interface vlan1

SWC(config-if)# ip address 10.1.1.60 255.255.255.0 (dirección IP de ejemplo)

* + Repetir los pasos anteriores para el conmutador D.

**Tarea 4:** Configuración de las interfaces de los conmutadores de acceso para que no se permita más de una dirección MAC por puerto de usuario. Para ello seguir los pasos siguientes:

* Paso 4.1: Entrar en conmutador C.
* Paso 4.2: Activar la seguridad de los puertos en todas las interfaces de acceso:

SWC(config)# interface range f0/1 – 22 (Atención con el rango que se selecciona)

SWC(config-if-range)# switchport mode access

SWC(config-if-range)# switchport port-security

* Paso 4.3: Visualizar cómo queda la configuración de la seguridad de los puertos a través del comando siguiente:

SWCA# show port-security interface f0/1 (para el Puerto fa/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 : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

Fijarse en los campos señalados, **¿qué nos indican?.**

* Paso 4.4: En el puerto fa0/1 del conmutador C, realizar el siguiente cambio: desconectar del conmutador el PC-C1, conectar en ese mismo puerto un *HUB* y a un puerto del hub conectar el PC-C1 y un nuevo PC. Una vez conectados, realizar un ping desde cada uno de estos PCs a cualquier otro de la red. **¿Hay conectividad? ¿Debería haber? Dar una explicación.**
* Paso 4.5: Visualizar ahora el estado de la seguridad de este puerto utilizando el comando del paso 4.3. **¿Qué ha cambiado? Razonar lo que ha ocurrido.**
* Paso 4.6: Comprobar si hay algún mensaje en el servidor syslog. Para ello, acceder al servicio syslog del servidor siguiendo el siguiente camino:

Seleccionar servidor 🡪 Services 🡪 Syslog

* Paso 4.7: Volver a la situación inicial. Para ello tener en cuenta que una vez realizados los cambios, la interfaz debe desactivarse y volver a activarse administrativamente utilizando el comando “shutdown” y “no shutdown” respectivamente.

**Tarea 5:** Configuración de las interfaces de los conmutadores de acceso para permitir únicamente una dirección MAC por puerto de usuario asignada de **manera estática**. Para ello seguir los pasos siguientes:

* Paso 5.1: Entrar en el conmutador C.
* Paso 5.2: Configurar el puerto donde está conectado el PC-C2 de la siguiente forma:

SWC(config)# interface f0/2

SWC(config-if)# shutdown

SWC(config-if)# switchport port-security mac-address <MACdePC-C2>

SWC(config-if)# no shutdown

* Paso 5.3: Visualizar cómo queda la configuración de la seguridad de los puertos a través del comando del paso 4.3 y también del comando “show port-security address”
* Paso 5.4: Intercambiar la conexión del PC-C2 con PC-C1 y realizar un ping a un equipo conectado al conmutador D desde los PCs anteriores**. ¿Qué resultado se obtiene? ¿Hay conectividad? ¿Por qué?**
* Paso 5.5: Visualizar ahora el estado del puerto y los mensajes recibidos en el servidor syslog.
* Paso 5.6: Volver a la situación inicial.

**Tarea 6:** Configuración de las interfaces de los conmutadores de acceso para que sólo se permita una dirección MAC por puerto de usuario asignada de **manera automática**. Para ello seguir los pasos siguientes:

* Paso 6.1: Entrar en el conmutador D.
* Paso 6.2: Activar la seguridad de los puertos en todos los puertos de acceso:

SWD(config)# interface range f0/1 - 22

SWD(config-if-range)# switchport mode access

SWD(config-if-range)# switchport port-security

* Paso 6.3: Configurar la asignación automática a la dirección MAC del primer equipo que se conecte a los puertos de acceso:

SWD(config)# interface range f0/1 -22

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

* Paso 6.4: Realizar pings desde uno de los PCs conectados al conmutador D a cualquier PC de la red.
* Paso 6.5: Visualizar la configuración con los comandos indicados en el paso 5.3. **¿Qué ha cambiado?**
* Paso 6.6: **¿Qué ocurriría si ahora se desconectara el PC-D utilizado en el paso 6.4 y se conectara en el mismo puerto un PC con una dirección física distinta?**

**Tarea 7: Explicar las diferencias entre el método empleado en la tarea 5 y el empleado en la tarea 6 para el control de acceso a los puertos**. Para ello, se puede acceder a los manuales en línea publicados por Cisco Systems o a cualquier otro documento siempre que sea de una fuente fiable (indicar siempre la referencia utilizada).

**Tarea 8:** Se ha visto en esta práctica que se puede controlar el acceso a los puertos de los conmutadores a través de la dirección MAC de los equipos. Sin embargo, **¿qué ocurriría si se enmascarase una dirección física autorizada (*MAC spoofing*)?**

**Tarea 9:** **¿Se le ocurre alguna forma de mejorar el control de acceso a la red a nivel 2? ¿Conoce el estándar IEEE802.1X? Investigue utilizando bibliografía fiable si este estándar podría ayudar y cómo a mejorar el control de acceso a la LAN.**

**(Se acabó la práctica)**