**Ejercicio 3- Seguridad en DHCP**

En la red de la compañía XYZ se han producido varias incidencias producidas por ataques que han aprovechado las vulnerabilidades de DHCP (*Dynamic Host Configuration Protocol*). Con el objetivo de mitigar los ataques, se ha decidido implantar la contramedida de seguridad siguiente:

* Activar en los conmutadores LAN la funcionalidad *DHCP snooping*

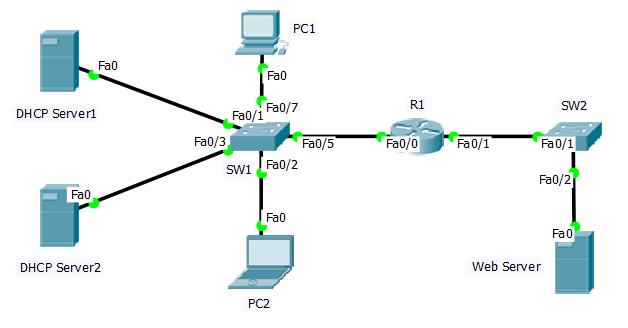


Figura 1. Topología de la red del ejercicio

**Guion de la práctica**

**Tarea 1:** Bajar el fichero de trabajo de la práctica desde Aula Digital. Al abril el fichero se podrá visualizar la red de la figura 1. Los sistemas de la red se deberán configurar siguiendo los pasos que en las siguientes tareas se irán indicando.

**Tarea 2:** Configurar el encaminador R1. Para ello, realizar los pasos siguientes:

* Paso 1. Pinchar sobre el encaminador y seleccionar la pestaña CLI
* Paso 2. La primera vez que se acceda al encaminador aparecerá en pantalla el texto siguiente:

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:

Escribir “n” y pulsar la tecla de “Intro”.

* Paso 3. Definir el nombre del encaminador siguiendo los pasos siguientes:

Router# config t (para entrar en la zona de configuración global)

Router(config)# hostname R1 (asigna el nombre R1)

R1(config)# exit

R1#

* Paso 4. Configurar las dos interfaces que se indican en la figura 1 de la forma siguiente:

R1#config t

R1(config)#interface fa 0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0 (asignación IP a interfaz)

R1(config-if)#no shutdown (activa interfaz)

R1(config-if)#interface fa 0/1

R1(config-if)#ip address 192.168.2.1 255.255.255.0 (asignación IP a interfaz)

R1(config-if)#no shutdown (activa interfaz)

R1(config-if)#exit

R1(config)#exit

R1#

* Paso 5. Comprobar que las dos interfaces están activas (*up*). Para comprobarlo, utilizar el comando siguiente:

R1#show ip interface brief

Analizar la información que aparece por pantalla.

Cuestión: ¿Sabría explicar la información que se visualiza?

R: Ambas interfaces han sido activadas de manera manual. La VLAN1 esta desactivada administrativamente.

De manera intuitiva, ¿puede indicar otra forma de ver si las interfaces están activas o no?

R:

* En la interfaz de la pestaña config.
* Por el color de la interfaz en el diagrama.
* Pasando el cursor por encima del router.

**Tarea 3:** Configurar el servidor DHCP número 1 (DHCP Server1):

* Paso 1. Configuración de los parámetros de la placa de red del servidor con los datos siguientes:
  + *Dirección ip: 192.168.1.2*
  + *Máscara de red: 255.255.255.0*
  + *Default Gateway: 192.168.1.1*

*Secuencia de configuración: Seleccionar DHCP Server1 🡪 Desktop 🡪 IP Configuration 🡪 rellenar datos*

* Paso 2. Configuración del servicio DHCP en DHCP Server1 con los datos siguientes:
  + *Start IP Address: 192.168.1.20*
  + *Default Gateway: 192.168.1.1*

*Secuencia:**Seleccionar DHCP Server1 🡪 Services 🡪 DHCP 🡪 Rellenar datos 🡪 SAVE 🡪 On 🡪 Cerrar ventana*

**Tarea 4:** Configurar PC1 y PC2 para que adquieran la configuración de red vía DHCP:

Secuencia: *Seleccionar PC 🡪 Desktop 🡪 IP configuration 🡪 seleccionar DHCP*

Una vez seleccionado el modo DHCP, comprobar que han adquirido automáticamente la configuración de los parámetros de red (*DHCP request successful*).

Cuestión: ¿Qué intercambio de mensajes se ha producido para que los PCs hayan adquirido la configuración ipv4 de manera automática a través de la red? Comparar la secuencia de este proceso que se visualiza a través del modo simulador de CPT con la teoría.

R: Coincide con la teoría. Se ejecuta DHCP DISCOVERY, DHCP OFFER, DHCP REQUEST y finalmente DHCP ACKNOWLEDGE. Esto se ha comprobado haciendo un ipconfig /release en el PC0 para eliminar su IP y entonces se ha activado el DHCP en IP configuration para que haga el proceso de obtención de una nueva IP address y esto se ha capturado con el modo simulación, seleccionando solo mensaje del tipo DHCP en los filtros de la simulación. Se adjunta una imagen(Hacer zoom para verlo bien):

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Tarea 5:** Configurar el servidor web (sólo hay que configurar los parámetros de red del ordenador o *host*, ya que el servicio HTTP ya está activado por defecto). Asignar la dirección ip 192.168.2.10 con máscara de clase C.

Secuencia de configuración: *Seleccionar Web server 🡪 Desktop 🡪 IP Configuration 🡪 configurar: ip address, Subnet mask y Default gateway*

**Tarea 6:** Comprobar desde PC1 y PC2 que hay comunicación con “Web Server” (primero utilizando la herramienta *ping* y después el navegador web).

Cuestión: ¿Qué se está comprobando realmente con cada una de las pruebas indicadas anteriormente? Argumentar la respuesta. Para ello, se puede utilizar la bibliografía recomendada u otra, siempre que ésta sea una fuente confiable. En cualquier caso, indicar siempre la fuente o fuentes consultadas.

R: se está comprobando que la configuración es correcta y que la tabla de encaminamiento y protocolo de encaminamiento del router funcionan correctamente.

**Tarea 7:** Configurar ahora el segundo servidor DHCP (DHCP Server2) con los datos siguientes:

* + *Dirección ip de la placa de red del servidor: 200.1.1.2 / Máscara de red: 255.255.255.0*
  + *Para el servicio DHCP:*
    - *Start IP Address: 200.1.1.10*
    - *Default Gateway: 192.168.1.1*

**Tarea 8:** Forzar peticiones DHCP desde PC0 o PC1 hasta conseguir que adquiera una configuración servida por el 2º servidor DHCP. Para ello, en el PC elegido, seleccionar “Static” y volver a seleccionar “DHCP” en la ventana de “IP Configuration” (repetir esta secuencia las veces que sea necesario hasta adquirir una configuración de la red 200.1.1.0/24). Una vez adquirida, repetir las mismas pruebas que se realizaron en la Tarea 6 y ver si ahora hay conectividad.

Cuestión: ¿Existe conectividad? ¿Debería de ser así? Describir lo que ha sucedido y dar una explicación.

R: No existe conectividad y así debe ser. Esto es porque la IP address obtenida del DHCP server2 no es de la misma subred que el default gateway que el PC0 tiene asignado, entonces el PC0 no puede comunicarse con el exterior(que es donde está precisamente el Web Server). De esta manera un atacante que coloca un DHCP server no legítimo puede conseguir un DoS (Denial of Service).

**Tarea 9:** Configuración de *DHCP snooping*. Para ello, proceder con los pasos siguientes:

* Paso 1: En el conmutador LAN SW1, activar *DHCP snooping* desde la zona de configuración global de la forma siguiente:

SW1> enable (Con el comando *enable* se accede a la zona con privilegios)

SW1# config terminal (Con este comando se accede a la zona de configuración. general)

SW1(config)# ip dhcp snooping

* Paso 2: Activar también *DHCP snooping* en vlan 1 (VLAN por defecto):

SW1(config)#ip dhcp snooping vlan 1

* Paso 3: Forzar nuevas peticiones DHCP desde cualquiera de los PCs (PC0/PC1).

Cuestión: ¿El PC adquiere la configuración de red servida por alguno de los servidores DHCP? ¿Esto es lo que debería ocurrir? Razonar la respuesta.

R: No, el PC0 por ejemplo, no adquiere la configuración. Esto es porque cuando se utiliza DHCP snooping, hay que establecer qué interfaces suen fiables (trust). Por defecto normalmente todas las interfaces son no trust, por lo tanto hasta que no asignemos una trust, el servicio DHCP será bloqueado por el conmutador.

Texto, Carta

Descripción generada automáticamente

* Paso 4: Configurar la interfaz “fa0/1” del SW1 como puerto autorizado (“trust”) de la forma siguiente:

SW1(config)#interface fa0/1 (atención, seleccionar interfaz donde esté conectado DHCP Server1)

SW1(config-if)#ip dhcp snooping trust

SW1(config-if)#exit

SW1(config)#exit

* Paso 5: Volver a forzar peticiones DHCP desde PC0. Mirar la configuración de red adquirida ahora por este PC y comprobar si hay conectividad con el servidor web.

Cuestión: ¿Podría dar una explicación del resultado que se ha obtenido? La ejecución del modo simulación puede ayudar a entender lo que sucede.

R: ahora tanto PC0 como PC1 obtienen direcciones ip a traves de DHCP. Pero solo a traves de DHCP server 1, ya que es el que cuelga de la interfaz del conmutador que hemos establecido como trust.

* Paso 6: Visualizar la configuración de *DHCP snooping* utilizando el comando siguiente:

SW1#show ip dhcp snooping

Cuestión: ¿Qué puertos aparecen en pantalla y en qué estado “trusted” está cada uno?

Texto

Descripción generada automáticamente

* Paso 7: Visualizar la tabla de *binding HW-IP address*:

SW1#show ip dhcp snooping binding

Cuestión: Describir la información que muestra esta tabla. ¿Las correspondencias “dirección MAC-dirección IP” son las que deberían ser?

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

R: esta tabla muestra las correspondencias MAC address – IP address de los terminales configurados con un DHCP conectado al switch. También indica el tiempo de validez de la ip asignada (86400 segundos), y la interfaz de la que cuelgan los terminales con estas MACs/IPs. Muestra también un número que representa el total de bindings que se encuentran en la tabla del conmutador. Las correspondencias MAC-dirección IP son correctas.

**Tarea 10:** Haga un breve resumen de la práctica (indicar los objetivos de la práctica, el resultado final obtenido y cómo se ha conseguido). ¿Qué tipo de ataque o ataques se han evitado/mitigado con la contramedida implementada?

R: Esta práctica permite aprender las vulnerabilidades existentes en el entorno DHCP. Hemos estudiado 2 ataques: Agotamiento de pool de direcciones DHCP y Colocación de un DHCP no legítimo. Las contramedidas aplicadas han sido DHCP snooping.

**(Se acabó la práctica)**