**21754 - Seguridad en Redes y Servicios**

Ejercicio práctico global

En la red de la empresa XYZ (ver figura 1), después de investigar los efectos de una serie de ataques informáticos detectados, se ha descubierto lo siguiente:

* Existencia de un servidor DHCP intruso en la red que ofrece configuraciones de red erróneas
* Modificación en el servidor DHCP corporativo que provoca en los equipos finales una carga automática de la configuración de red errónea.
* Existencia de un encaminador en la red de interconexión que interconecta una red intrusa a la red corporativa.

El responsable de seguridad de la empresa le ha encargado al equipo TIC que solucione esta situación y realice las actuaciones necesarias en la red que eviten que vuelva a producirse.

Por otro lado, hay que conectar la red de una oficina remota (con 4 PCs de usuario) a la red central de la manera más segura y económica. Esta oficina no aparece en el esquema de la figura 1 ya que es nueva.

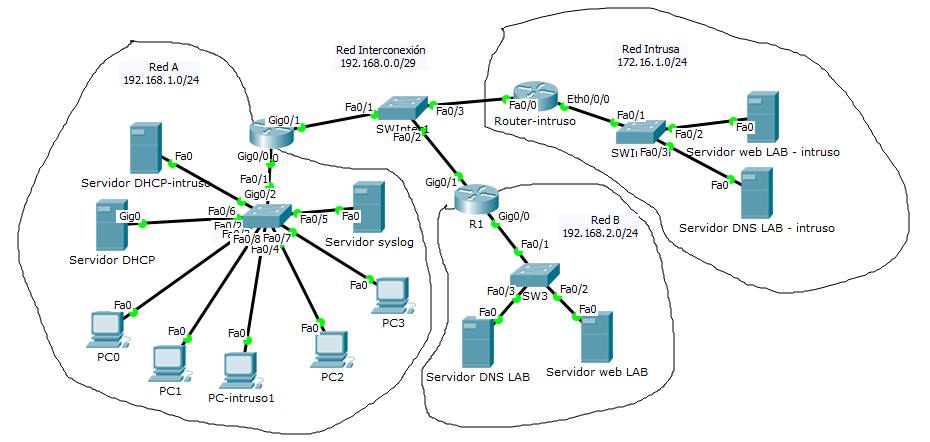


Figura 1. Esquema de la red de la empresa XYZ

**Guion del ejercicio:**

**Primera parte. Obtención del fichero de trabajo y estudio de la situación inicial**

**Tarea 1: Esquema de direccionamiento.** Obtener el fichero CPT de trabajo del espacio de Aula digital. A partir de la configuración inicial de la red (ver figura 1), completar la tabla 1. *[0,5 puntos sobre 10]*

Tabla 1. Esquema de direccionamiento IP de la red de la empresa XYZ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivo** | **Interfaz** | **Dirección IPv4/máscara de red** | **Router predeterminado** | **Servicios activos** |
| R0 | Gig0/0 | 192.168.1.1 / 255.255.255.0 | - | - |
|  | Gig0/1 | 192.168.0.1 / 255.255.255.248 | - | - |
| R1 | Gig0/0 | 192.168.2.1 / 255.255.255.0 | - | - |
|  | Gig0/1 | 192.168.0.2 / 255.255.255.248 | - | - |
| Router intruso | FastEthernet0/0 | 192.168.0.3 / 255.255.255.248 | - | - |
|  | Eth0/0/0 | 172.16.1.1 / 255.255.255.0 | - | - |
| PC0 | FastEthernet0 | 192.168.1.52 / 255.255.255.0 | 192.168.1.1 | - |
| PC3 | FastEthernet0 | 192.168.1.15 / 255.255.255.0 | 192.168.1.1 | - |
| PC-Intruso1 | FastEthernet0 | 192.168.1.9 / 255.255.255.0 | 192.168.1.1 | - |
| SW1 | Vlan 1 | 192.168.1.20 / 255.255.255.0 | - | - |
| Servidor web LAB | Gig0 | 192.168.2.8 / 255.255.255.0 | 192.168.2.1 | HTTP |
| Servidor web LAB - intruso | FastEthernet0 | 172.16.1.8 / 255.255.255.0 | 172.16.1.1 | HTTP |
| Servidor DNS LAB | FastEthernet0 | 192.168.2.4 / 255.255.255.0 | 192.168.2.1 | DNS |
| Servidor DNS LAB-intruso | FastEthernet0 | 172.16.1.4 / 255.255.255.0 | 172.16.1.1 | DNS |
| Servidor syslog | FastEthernet0 | 192.168.1.3 / 255.255.255.0 | 192.168.1.1 | SYSLOG |
| Servidor DHCP | Gig0 | 192.168.1.4 / 255.255.255.0 | 192.168.1.1 | DHCP |
| Servidor DHCP-intruso |  | 172.16.1.5 / 255.255.255.0 | 172.16.1.1 | DHCP |

**Tarea 2: Estado actual de la red de la empresa**. Analizar el estado en el que se encuentra actualmente la red de la empresa. Responder a las siguientes preguntas: ¿Qué **equipos** y **zonas** se han visto afectadas? Indicar todos los **efectos (tipos de ataques)** que se aprecian en el funcionamiento de la red. *[0,5 puntos sobre 10]*

Efectos (tipos de ataques) que se aprecian:

Red A

* Servidor DHCP furtivo. Los equipos de la red A que han sido afectados son:
* PC0.
* PC1.
* PC2.

Estos 3 PCs, que tienen configuración de ip a través de DHCP, han obtenido una dirección ip del servidor DHCP furtivo, en lugar de obtenerla del servidor DHCP legítimo.

* El ataque de Servidor DHCP furtivo provoca a la vez un ataque de DoS (Denegación de servicio), ya que los PCs 0, 1 y 2, que han obtenido direcciones ip del servidor malicioso de manera que han quedado colocados en la subred 172.16.1.0, no tienen conectividad con el resto de equipos de la subred que han obtenido una dir. Ip del servidor legítimo, perteneciendo entonces a la subred 192.168.1.0. Para comunicar 2 subredes, hay que pasar por un router, pero como el router R0 no tiene en la tabla de encaminamiento la entrada que corresponderia a esta comunicación (porque en la red original, sin que hubiera sido afectada por intrusos, no tiene sentido que exista esta entrada), no hay conectividad.

Por otra parte, a los PCs 0, 1 y 3 también se les ha asignado un **default gateway** incorrecto, por lo que sus datos **ni siquiera pueden salir de su propia subred**.

* Ataque MAC Flooding. NO ha ocurrido aún, pero como se ha conectado un PC intruso a la red, y la interfaz a la que se ha conectado no tiene port-security activado, el PC intruso podría enviar muchas direcciones MAC falsas y provocar un desbordamiento de la tabla de MACs del switch de la Red A:

**Texto

Descripción generada automáticamente**

* Aunque haya equipos que tienen asignado el servidor DNS legítimo, como el PC3, estos también podrían verse afectados, ya que el PC-intruso1, que tiene asignado el servidor DNS legítimo también, podría realizar un ataque DoS enviando un número muy grande de **bogus queries** u otro tráfico, desbordando su capacidad y provocando que no pueda responder a las peticiones legítimas de por ejemplo el PC3.

Red intrusa

* Ataque Man-in-the-middle: se ha provocado que los equipos de la red A sean redirigidos a la red intrusa en lugar de a la red legítima cuando realizan consultas web. Con la confuguración DHCP del servidor no legítimo, se les ha asignado el servidor DNS también no legítimo, y este servidor tiene una resolución de nombres que envia la petición al servidor web LAB-intruso, en lugar de al Servidor web LAB legítimo. La petición web de los clientes parecerá ser correcta desde su perspectiva, cuando en realidad, sin saberlo, están siendo redirigidos a la red intrusa.

**Segunda parte. Buscar soluciones para la protección de la red**

**Tarea 3.** **Vulnerabilidades.** Indicar y describir brevemente las **vulnerabilidades** que han podido facilitar el ataque o ataques producidos en la red de la empresa XYZ. *[1 punto sobre 10]*

Las vulnerabilidades que han facilidado los ataques y amenazas son las siguientes:

* No haber configurado puertos trust para aceptar DHCPoffer solo por esa vía.
* No haber configurado port-security en las interfaces del Switch de la red A.

**Tarea 4.** **Posibles soluciones.** Indicar y describir brevemente qué **medidas** (del temario de la asignatura) se podrían aplicar para conseguir el **objetivo** marcado por el responsable de seguridad de la empresa. Para cada una de las medidas, **razonar/justificar su uso**.  *[1 punto sobre 10]*.

Medida 1: Configurar DHCP snooping.

Razón: para mitigar los ataques DHCP Furtivo y agotamiento de direcciones DHCP.

Justificación: para el problema del agotamiento de direcciones DHCP, si se limitan el número de MACs que pueden aparecer por interfaz LAN (**switchport port-security maximum 1**), se podría evitar el problema. El presunto atacante quedaría bloqueado (shutdown de interfaz) cuando intentara utilizar más de una dirección MAC. Sin embargo esto no bastaría, ya que los servidores DHCP no utilizan la dirección MAC de la trama Ethernet para asignar direcciones, sino la que aparece dentro del mensaje BOOTP/DHCP, que no es vista por un conmutador común. Con DHCP snooping, se permite a los conmutadores inspeccionar la información contenida dentro de los mensajes DHCP.

DHCP snooping permite al conmutador comprobar si la dirección MAC dentro del paquete DHCP coincide con la de la cabecera Ethernet, si no coincide el paquete de puede desactivar o desactivar la interfaz LAN.

Además, el conmutador aprovecha esta funcionalidad para construir una tabla, llamada DHCP binding table que le permite disponer de la correspondencia entre las direcciones MAC e IP asignadas.

Por otra parte, para combatir el servidor DHCP furtivo, se deberían aceptar solo los mensajes DHCPOffer cuando vengan de puertos donde se sabe que hay servidores legítimos.

**Tercera parte. Implementación de las medidas de protección**

**Tarea 5: Implementar las medidas de seguridad apropiadas.** Realizar la **configuración** necesaria en los sistemas de la red para **proteger** la red de las **vulnerabilidades** que se han detectado como las facilitadoras del ataque de seguridad que se ha producido en la red de la empresa. Describir brevemente los **pasos realizados** para cada una de las técnicas. *[2 puntos sobre 10]*

**Para implementar DHCP snooping, los pasos realizados han sido los siguientes:**

1. **Activar DHCP snooping en el conmutador LAN SW1 desde la zona de configuración global:**

**# ip dhcp snooping.**

**# ip dhcp snooping vlan 1.**

1. **Configurar la interfaz “fa0/6” del SW1 como puerto autorizado(“trust”):**



1. **En el servidor DHCP legítimo, cambiar el servidor DNS en Servicios > DHCP ya que aunque ahora con el DHCP snooping los equipos de la red A siempre reciben la configuración del servidor DNS legítimo, este aún estaba configurado para asignar el servidor DNS ilegítimo:**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Tarea 6: Verificación y comprobación.** Para cada una de las medidas llevadas a cabo, indicar cómo se ha **comprobado** su funcionamiento y cómo puede **verificarse** que la configuración es correcta. *[1 punto sobre 10]*

**Comprobación y verificación para DHCP snooping:**

1. **Tras realizar la configuración, se ha comprobado su efecto mostrando el resultado con el comando “show ip dhcp snooping”:**

Tabla

Descripción generada automáticamente

1. **Tras realizar la configuración, se han forzado peticiones DHCP desde los equipos de la red A para ver la nueva configuración de red adquirida.**
2. **Al consultar la configuración de red de estos equipos, se verifica que el funcionamiento es correcto, siempre la reciben del servidor DHCP legítimo:**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Cuarta parte. Nueva oficina remota**

**Tarea 7: Crear la red de la nueva oficina remota y realizar la interconexión con la red central.** Se tiene que definir el direccionamiento ip de la nueva red, añadirla a la red de la figura 1 y realizar las comprobaciones básicas para comprobar que existe **conectividad**. Describir brevemente los **pasos** realizados. *[1 punto sobre 10]*

**Pasos realizados:**

1. **Colocación del hardware que compone la nueva red, y conexión de esta con el switch de la red de interconexión:**

Diagrama, Esquemático

Descripción generada automáticamente

1. **Definición del direccionamiento ip (configuración estática en este caso) para los 4 pcs de la nueva subred y las 2 interfaces del nuevo router. Elección de la subred 192.168.3.0/24 para la oficina. Las direcciones ip se han asignado mediante las interfazes de configuración:**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. **Activación de las 2 interfaces del Router0 con el comando “no shutdown”.**
2. **Activación del protocolo de encaminamiento OSPF en el router0 (Sin esto, los pings a otras subredes fallaban y se podia ver que la tabla de encaminamiento del nuevo router estaba incompleta). Esto se ha hecho de la siguiente manera:**





Texto

Descripción generada automáticamente



1. **Inspección de la tabla de encaminamiento actualiazada. Ahora parece estar completa:**

Interfaz de usuario gráfica, Texto, Aplicación, Tabla

Descripción generada automáticamente

1. **Realización de varios pings a otras subredes. Funcionan, ahora hay conectividad.**

**Un ejemplo, ping desde el PC5 de la oficina al PC0 de la Red A:**

Texto

Descripción generada automáticamente

**Tarea 8: Configurar el enlace seguro entre las dos redes.** Realizar la **configuración** necesaria para crear una **VPN** entre las dos redes. Una vez configurada, realizar las **verificaciones** y **comprobaciones** del funcionamiento. Describir brevemente los **pasos** realizados. *[3 puntos sobre 10]*

**(Se acabó el ejercicio)**