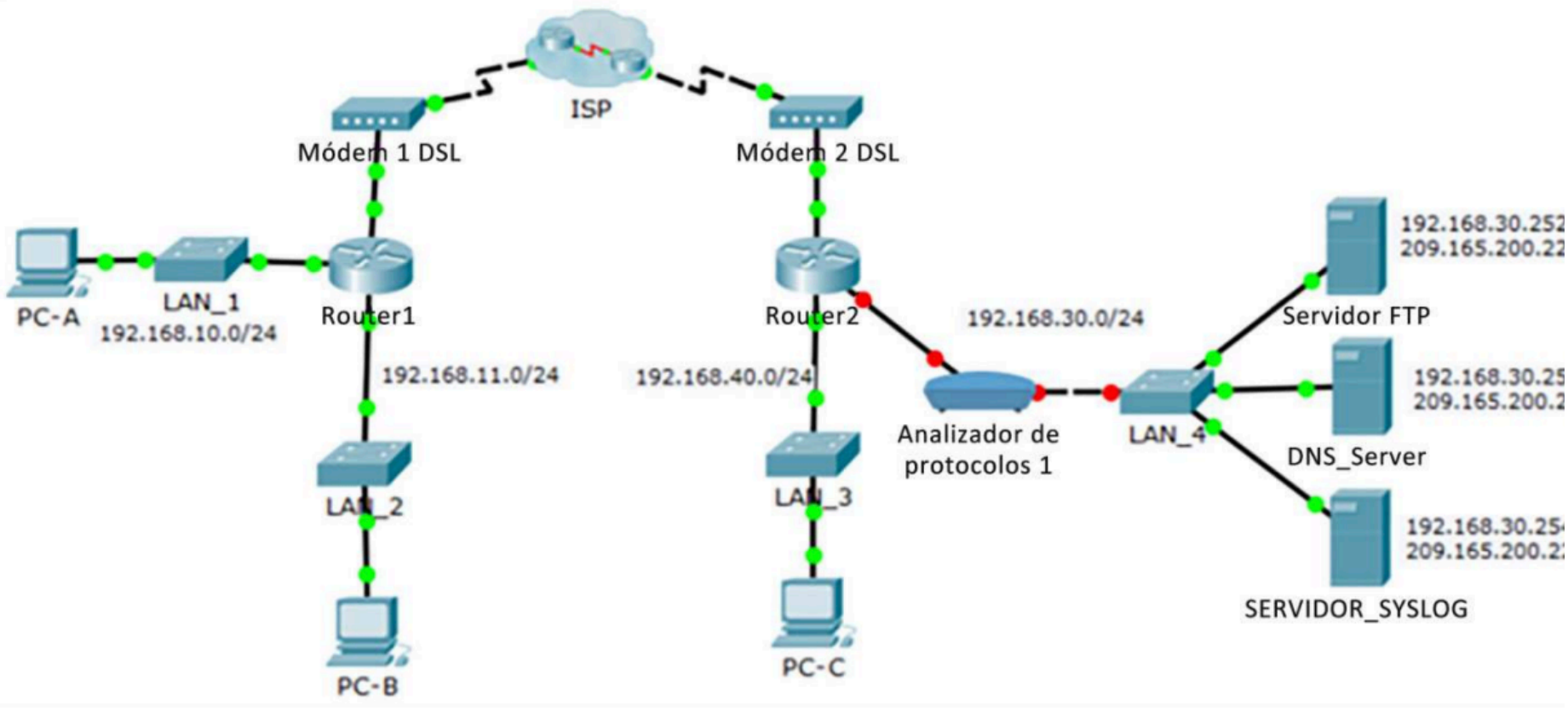
7.1.2.7 Packet Tracer: Registrar la actividad de la red

Topología



Descripción

Tabla de asignación de direcciones

El administrador	Dirección IP privada	Dirección IP pública
FTP_Server	192.168.30.253	209.165.200.227
SYSLOG_SERVER	192.168.11.254	209.165.200.229
Router2	N/D	209.165.200.226

Objetivos

Parte 1: Crear tráfico de FTP.
Parte 2: Investigar el tráfico de FTP.
Parte 3: Ver mensajes de Syslog

Aspectos básicos

En esta actividad utilizarán Packet Tracer para analizar y registrar el tráfico de red. Verán una vulnerabilidad de seguridad en una aplicación de red, y el tráfico ICMP registrado con syslog.

Parte 1: Crear tráfico de FTP

Paso 1: Activar el dispositivo analizador

a. Hagan clic en el dispositivo analizador **Sniffer1**.

b. Diríjanse a la ficha **Physical** (Físico) y enciendan el analizador.

c. Diríjanse a la ficha **GUI** y activen el servicio del analizador.

d. Se están monitoreando los paquetes FTP y syslog que ingresan al analizador desde Router2.

Paso 2: Conéctense de manera remota al servidor FTP.

a. Hagan clic en **PC-B** y diríjanse al escritorio.

b. Hagan clic en el **Símbolo del sistema**. En el símbolo del sistema, abran una sesión de FTP con **FTP_SERVER** utilizando su dirección IP pública. Se pueden consultar la Ayuda de la línea de comandos si se escribe **?** en el cursor.

c. Introduzcan **cisco** como nombre de usuario y **cisco** como contraseña para autenticarse con el **FTP_Server**.

Paso 3: Cargar un archivo al servidor FTP

a. En el indicador de **ftp>**, introduzca el comando **dir** para ver los archivos almacenados actualmente en el servidor FTP remoto.

b. Carguen el archivo **clientinfo.txt** en el servidor FTP; para ello, introduzcan el comando **put clientinfo.txt**.

c. En el indicador de **ftp>**, introduzca el comando **dir** y verifique que el archivo **clientinfo.txt** ahora esté en el servidor FTP.

d. Escriban **quit** en el cursor de FTP para cerrar la sesión.

Parte 2: Investigar el tráfico de FTP

a. Hagan clic en el dispositivo **Sniffer1** y, luego, en a ficha **GUI**.

b. Hagan clic en algunos de los primeros paquetes FTP de la sesión. Recuerden desplazarse hacia abajo para ver la información sobre el protocolo de capa de aplicación en los detalles de cada paquete. (Se asume que es su primera sesión FTP. Si han abierto otras sesiones, limpien la ventana y repitan el proceso de inicio de sesión y transferencia de archivos.)

¿Cuál es la vulnerabilidad de seguridad que presenta FTP?
¿Qué debe hacerse para mitigar esta vulnerabilidad?

Parte 3: Ver mensajes de syslog

Paso 1: Conectarse en forma remota a Router2

a. Desde la línea de comando de **PC-B**, ejecuten telnet a **Router2**.

b. Utilicen **ADMIN** como nombre de usuario y **CISCO** como contraseña para la autenticación.

c. Introduzcan los siguientes comandos en el cursor del router:

```
Router2# debug ip icmp
```

d. Escriban **logout** en el cursor para cerrar la sesión de Telnet.

Paso 2: Generar y ver mensajes de syslog

a. Hagan clic en el dispositivo **SYSLOG_SERVER** y diríjanse a la ficha **Services** (Servicios).

b. Hagan clic en el servicio **SYSLOG**. Verifiquen que el servicio esté activado. Los mensajes de syslog aparecerán aquí.

c. Diríjanse al host PC-B y abran la ficha **Desktop** (Escritorio).

d. Abra el **indicador de comando** y haga **ping** a Router2.

e. Diríjanse al host PC-A y abran la ficha **Desktop**.

f. Diríjase al indicador de comando y haga **ping** a Router2.

g. Investiguen los mensajes registrados en el servidor syslog.

h. Debería haber cuatro mensajes de PC-A y cuatro de PC-B. ¿Pueden decir qué respuestas echo son para PC-A y para PC-B a partir de las direcciones de destino? Expliquen.

i. **Hagan** ping a Router2 desde PC-C.

¿Cuál será la dirección de destino para las respuestas?