

## Packet Tracer: Registrar la actividad de la red

### Tabla de direccionamiento

Dispositivo	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/Situación.

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

### Instrucciones

#### Parte 1: Crear tráfico de FTP

##### Paso 1: Activar el dispositivo analizador

- Haga clic en el dispositivo analizador **Sniffer1**.
- Diríjase a la ficha **Physical** (Físico) y encienda el analizador.
- Diríjase a la ficha **GUI** y active el servicio del analizador.
- Se están monitoreando los paquetes FTP y syslog que ingresan al analizador desde Router2.

##### Paso 2: Conectarse de manera remota al servidor FTP.

- Haga clic en **PC-B** y diríjanse al escritorio.
- Haga clic en **Command Prompt**. En el símbolo del sistema, abra una sesión de FTP con **FTP\_SERVER** utilizando la dirección IP pública del dispositivo. Se pueden consultar la Ayuda de la línea de comandos si se escribe ? en el prompt (prompt es la linea de comandos).
- Introducir **cisco** como nombre de usuario y **cisco** como contraseña para autenticarse con el **FTP\_Server**.

##### Paso 3: Cargar un archivo al servidor FTP

- En el prompt de **ftp>**, introduzca el comando **dir** para ver los archivos almacenados actualmente en el servidor FTP remoto.
- Cargue el archivo **clientinfo.txt** en el servidor FTP; para ello, introduzca el comando **put clientinfo.txt**.

- c. En el prompt de **ftp>**, introduzca el comando **dir** y verifique que el archivo **clientinfo.txt** ahora esté en el servidor FTP.
- d. Escribir **quit** en el prompt de FTP para cerrar la sesión.

## Parte 2: Investigar el tráfico de FTP

- a. Haga clic en el dispositivo **Sniffer1** y, luego, en la ficha **GUI**.
- b. Haga clic en algunos de los primeros paquetes FTP de la sesión. Recordar 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 se han abierto otras sesiones, limpiar la ventana y repetir 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**, ejecutar telnet a **Router2**.
- b. Utilizar **ADMIN** como nombre de usuario y **CISCO** como contraseña para la autenticación.
- c. Introducir los siguientes comandos en el prompt del router:  
**Router2# debug ip icmp**
- d. Escribir **logout** en el cursor para cerrar la sesión de Telnet.

### Paso 2: Generar y ver mensajes de syslog

- a. Haga clic en el dispositivo **SYSLOG\_SERVER** y diríjanse a la ficha **Services** (Servicios).
- b. Haga clic en el servicio **SYSLOG**. Verificar que el servicio esté activado. Los mensajes de syslog aparecerán aquí.
- c. Dirigirse al host PC-B y abrir la ficha **Desktop** (Escritorio).
- d. Abrir el **Command Prompt** y hacer **ping** a Router2.
- e. Dirigirse al host PC-A y abrir la ficha **Desktop**.
- f. Dirigirse al Command Prompt y hacer **ping** a Router2.
- g. Investigar los mensajes registrados en el servidor syslog.
- h. Debe haber cuatro mensajes de PC-A y cuatro de PC-B.  
¿Podemos definir cuáles respuestas de tipo echo, pertenecen a la PC-A y a la PC-B a partir de las direcciones de destino? Explique.r sus respuestas aquí.
- i. **Hacer ping a Router2 desde PC-C.**  
¿Cuál será la dirección de destino para las respuestas?