**Packet Tracer: la comunicación en un mundo cibernético**

Parte 1: Enviar correo electrónico entre los usuarios

Paso 1: Acceda al correo electrónico del cliente en la computadora Mike

.

a. Haga clic en Gotham Healthcare Branch y luego haga clic en la computadora Mike.

b. Haga clic en la ficha Escritorio y luego haga clic en Correo electrónico.

Paso 2: Envíe un correo electrónico a Sally.

a. Cree un correo electrónico al hacer clic en el botón Redactar.

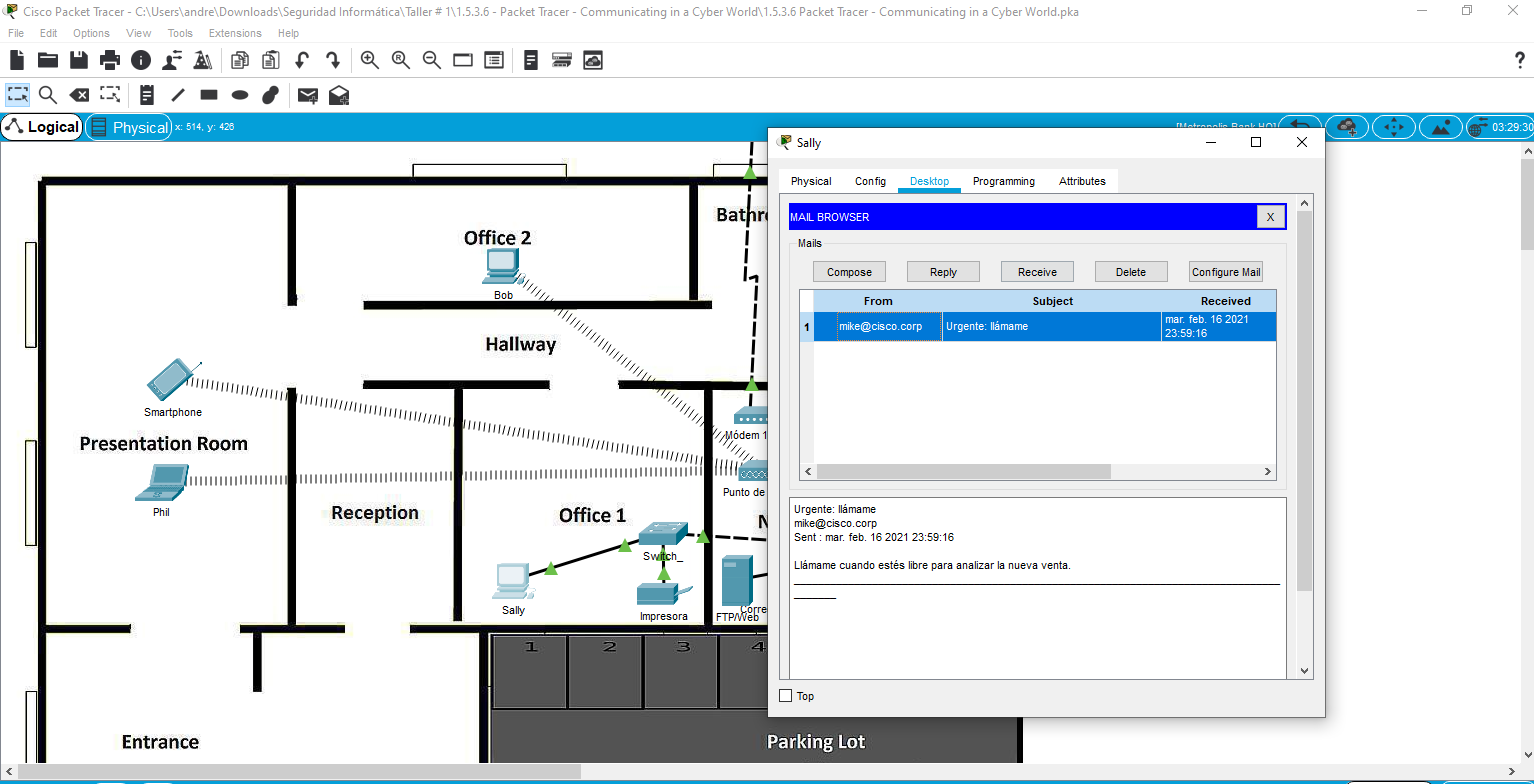
b. En el campo Para:, introduzca el correo electrónico sally@cisco.corp En el campo Asunto: , introduzca la cadena de texto «Urgente: llámame». En la sección Mensaje, introduzca. «Llámame cuando estés libre para analizar la nueva venta.»

c. Haga clic en el botón Enviar para transmitir el correo electrónico.

¿Qué protocolo se utilizó para enviar de correo electrónico al servidor de correo electrónico?

SMTP

Paso 3: Haga que Sally verifique su correo electrónico. a. Ingrese al sitio de Metropolis Bank HQ y luego haga clic en la computadora Sally. b. Haga clic en la ficha Escritorio y luego haga clic en Correo electrónico. c. Haga clic en el botón Recibir para recuperar el correo electrónico enviado desde la computadora Mike.



¿Qué protocolo se utilizó para enviar el correo electrónico desde el servidor de correo electrónico?

POP3

Parte 2: Cargar archivos mediante FTP

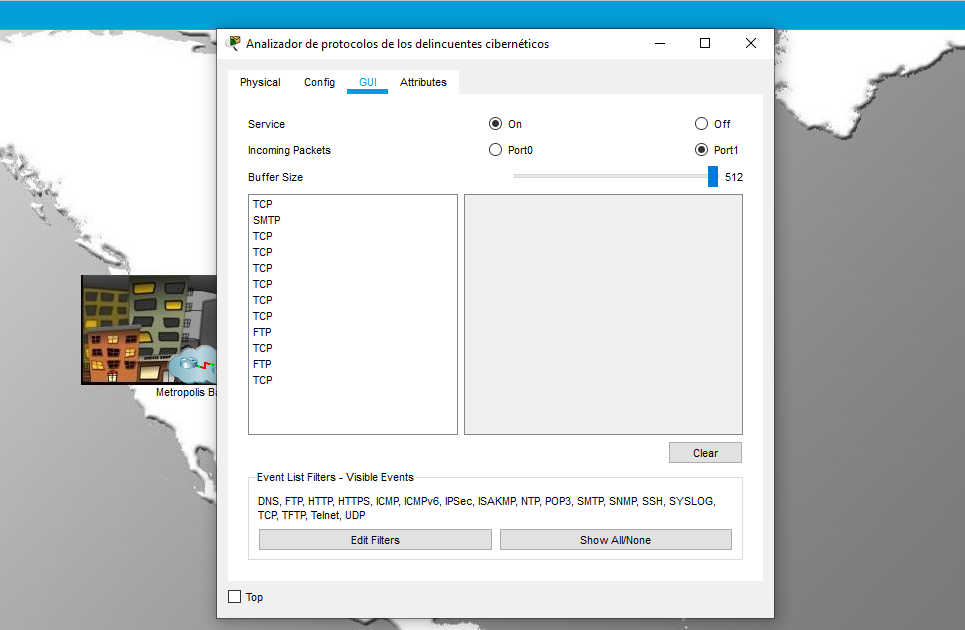
Paso 1: Establezca el analizador de protocolos de paquetes para capturar el tráfico en el puerto correcto.

a. Ingrese la vista geográfica (raíz) para ver los tres sitios remotos.

b. Haga clic en Analizador de protocolos de delincuentes cibernéticos.

c. Haga clic en Puerto1 para capturar paquetes de este puerto.

d. Deje abierta y visible la opción Analizador de protocolos de delincuentes cibernéticos para el resto de esta parte.



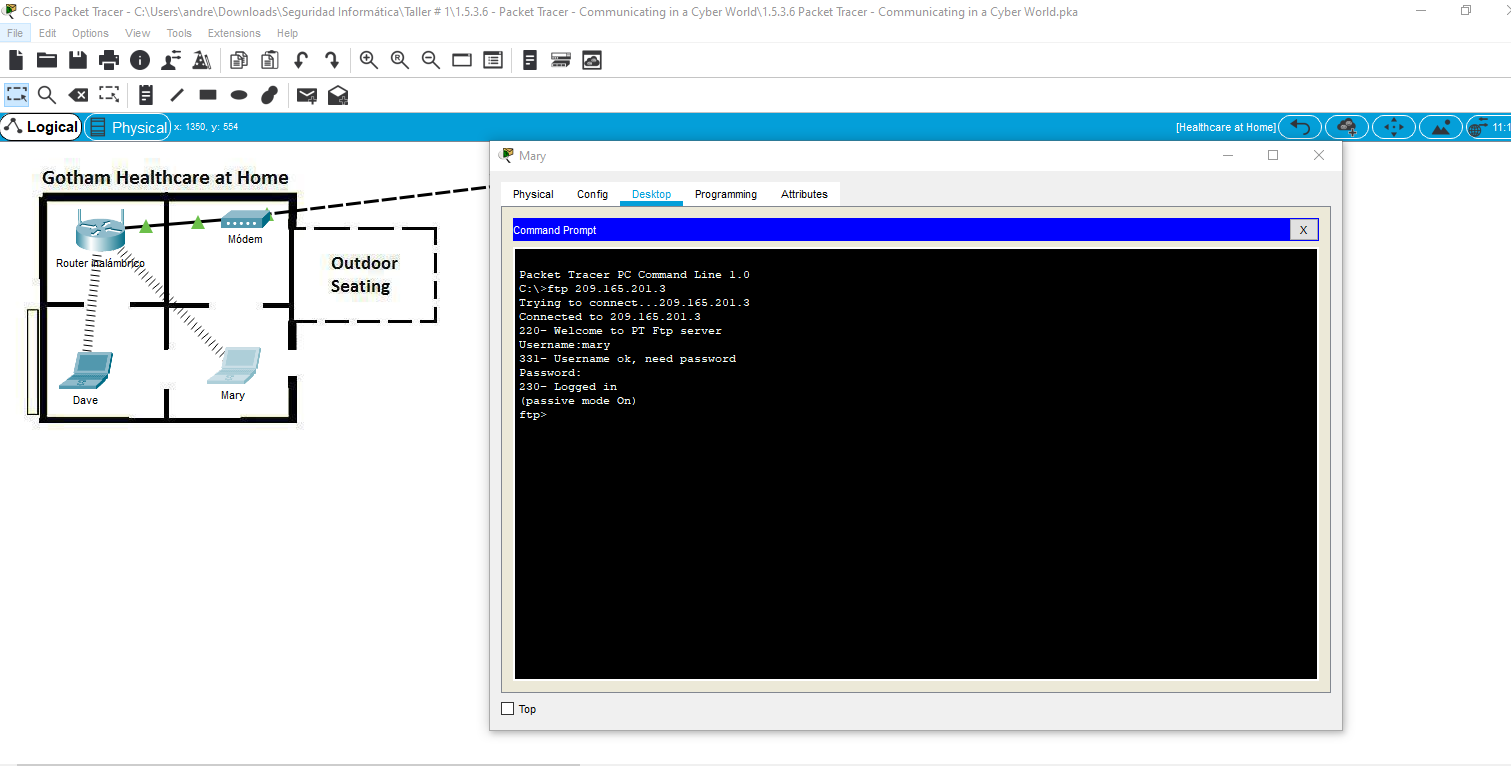
Paso 2: Conéctese de manera remota al servidor FTP.

a. Introduzca el sitio Healthcare at Home y luego haga clic en la computadora Mary.

b. Haga clic en la ficha Escritorio y luego haga clic en Petición de ingreso de comando.

c. Conéctese al servidor FTP/Web enMetropolis Bank HQ al introducir ftp 209.165.201.3 en la petición de ingreso de comandos.

d. Introduzca el nombre de usuario de mary y la contraseña cisco123.



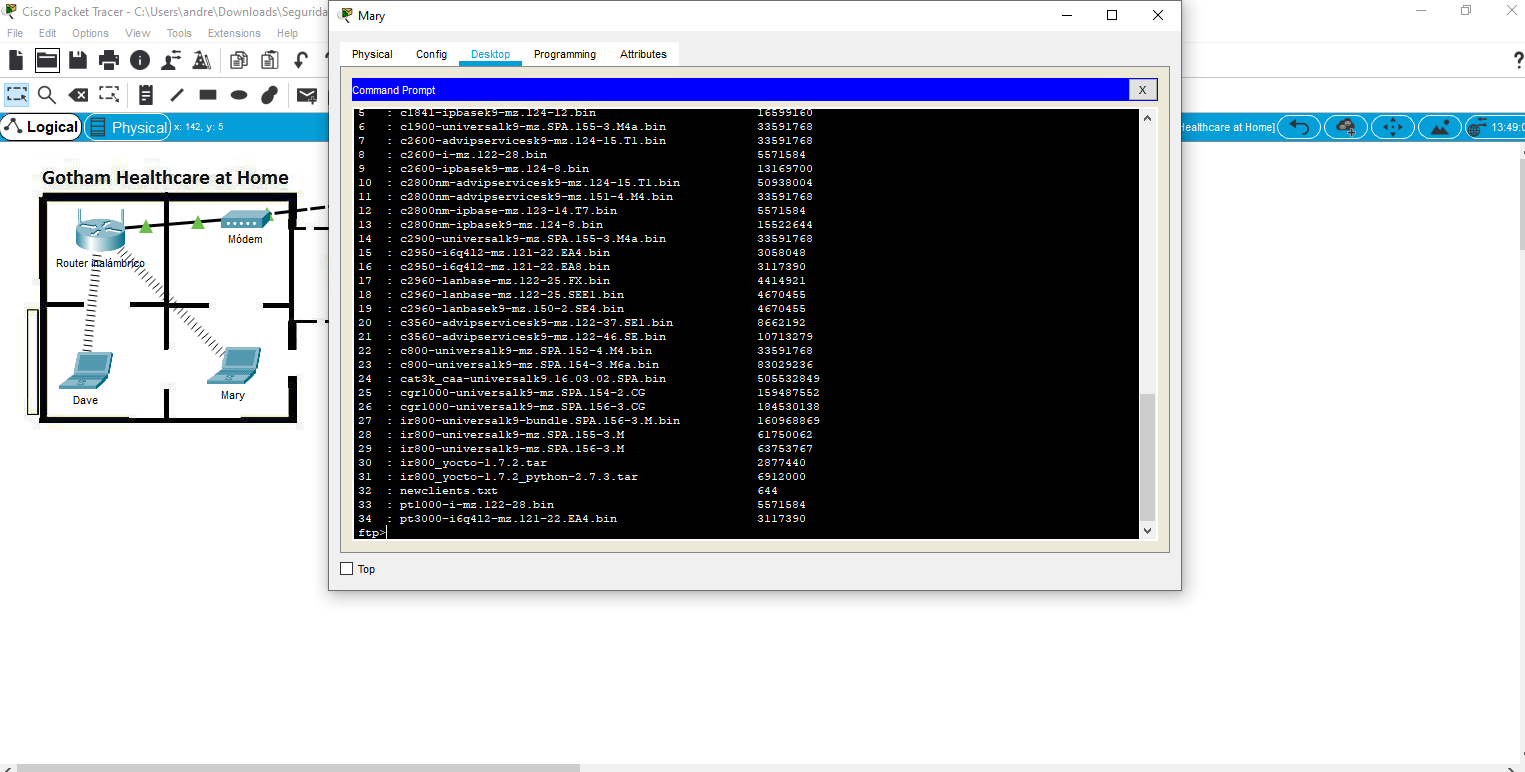
Paso 3: Subir un archivo al servidor FTP.

a. En el indicado

rftp>, introduzca el comando dir para ver los archivos actuales almacenados en el servidor FTP remoto.

b. Mary tiene un archivo que contiene información confidencial con respecto a la nueva información de servicios de salud del cliente. Cargue el archivo newclients.txt en el servidor FTP al introducir el comando put newclients.txt.

c. En el indicador ftp>, introduzca el comando dir y verifique que el archivo newclients.txt ahora se encuentre en el servidor FTP.



¿Por qué el FTP se considera un protocolo inseguro para archivos móviles?

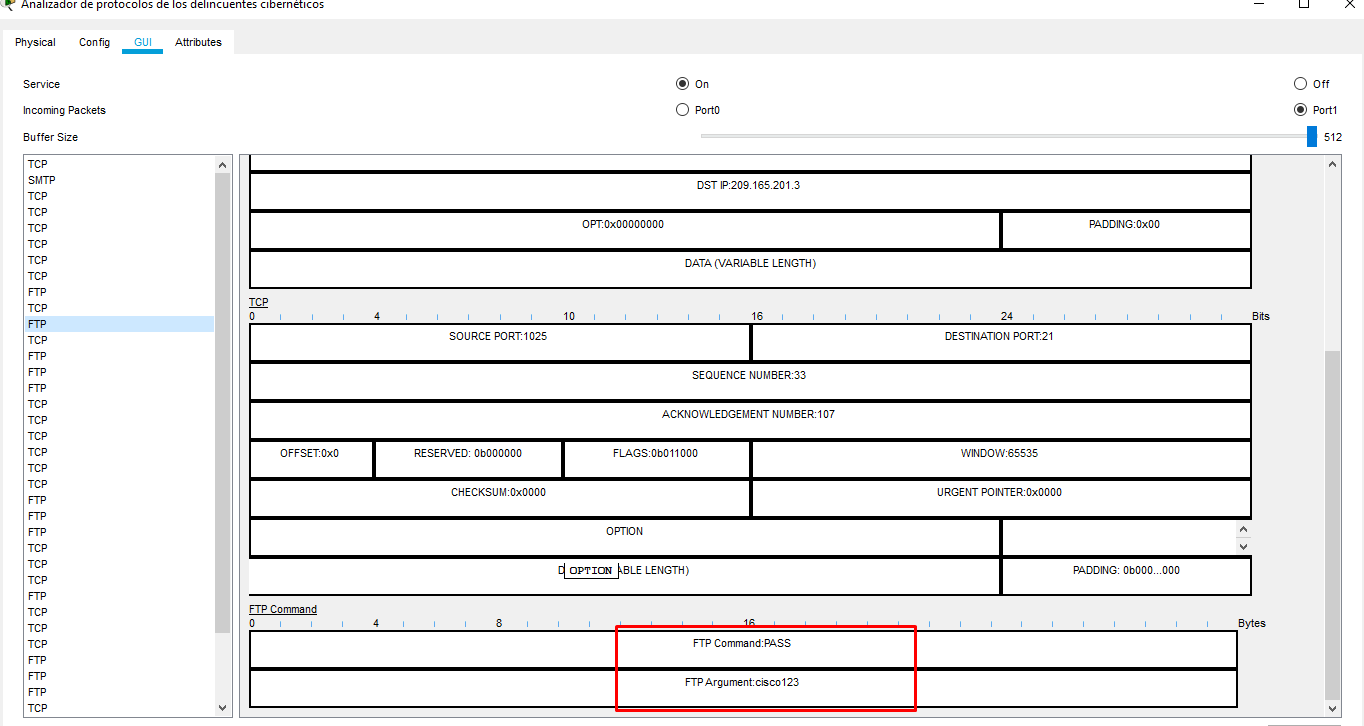
Ya no se considera seguro en la actualidad debido a su antigüedad ya no cumple los requisitos de seguridad de hoy, tanto el usuario como la contraseña se transmiten sin encriptar y esto puede representar una vulnerabilidad en mi sistema, actualmente se recomiendan SFTP y FTPS.

Paso 4: Analice el tráfico de FTP. a. Ingrese la vista geográfica (raíz) para ver los tres sitios remotos. b. Haga clic en Analizador de protocolos de delincuentes cibernéticos. c. En la ficha GUI a la izquierda, haga clic en el 1.° paquete de FTP disponible para seleccionarlo. Luego desplácese hasta la parte inferior de la ventana que se muestra a la derecha.

¿Qué información se muestra en el texto claro del encabezado del FTP?

El usuario, la IP y la contraseña, esto representa una vulnerabilidad por la cual otras personas podrían acceder a nuestro ordenador.

. Haga clic en el 2.° paquete de FTP disponible para seleccionarlo. Luego desplácese hasta la parte inferior de la ventana que se muestra a la derecha. Haga esto de nuevo para el 3.° paquete de FTP.



Además del nombre de usuario, ¿qué otra información confidencial se muestra en el texto claro del encabezado del FTP?

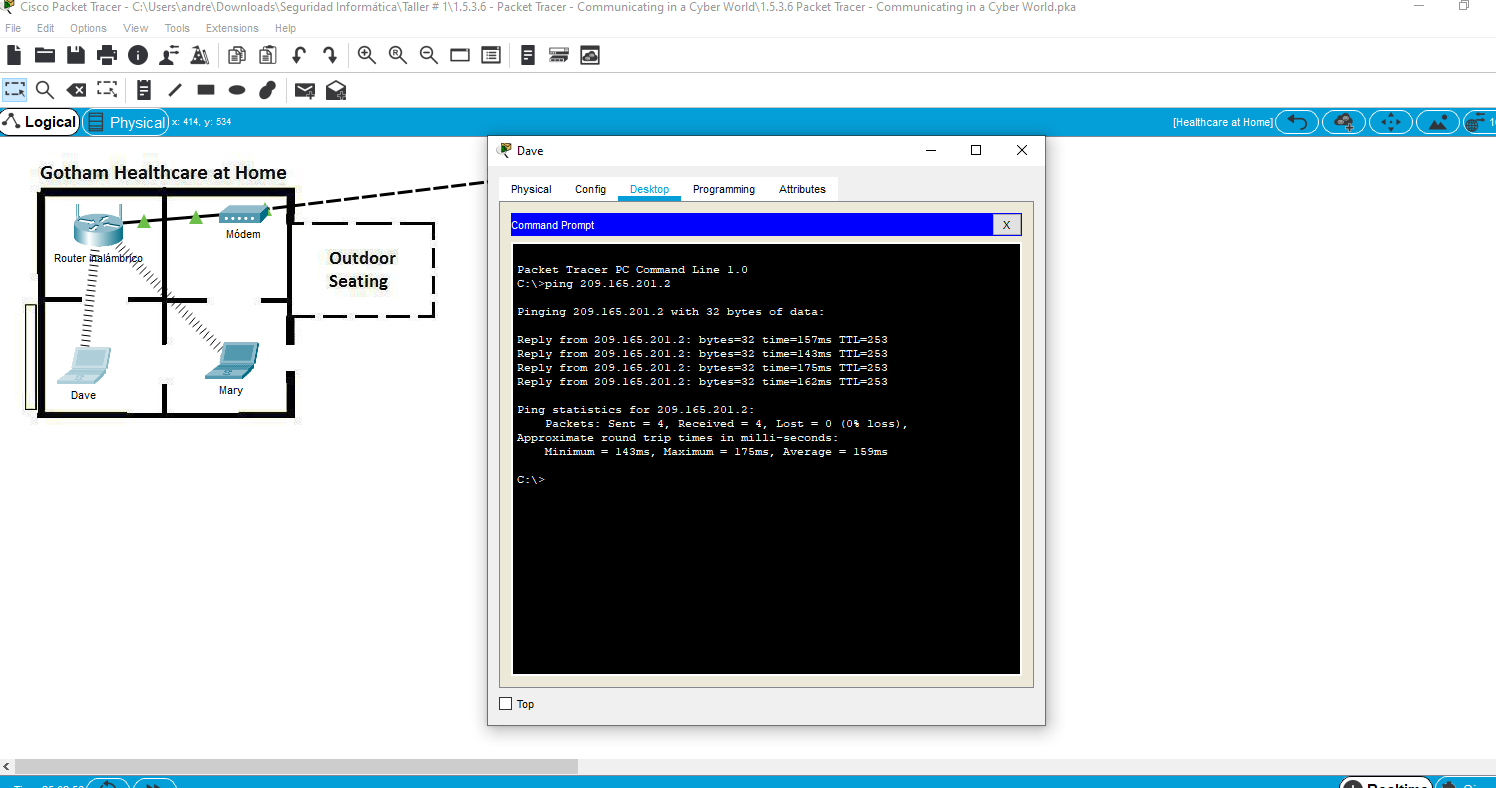
La IP y la contraseña, con esta información cualquier persona puede acceder a nuestro ordenador

Parte 3: Acceder de manera remota a un router de la empresa mediante Telnet Paso 1: Conéctese de manera remota al router de la empresa.

a. Ingrese al sitio Healthcare at Home y luego haga clic en la computadora Dave.

b. Haga clic en la ficha Escritorio y luego haga clic en Petición de ingreso de comando.

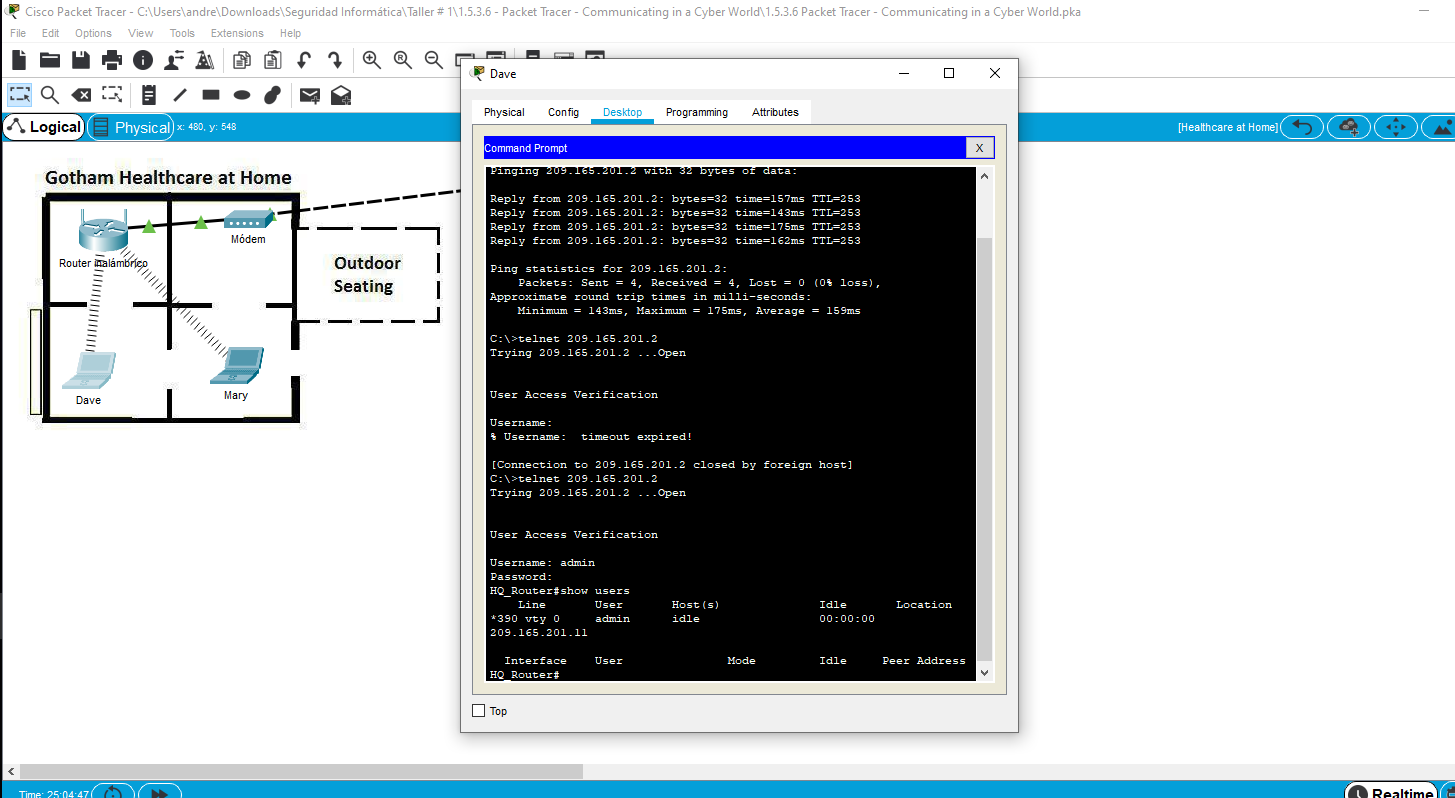
c. Haga ping al router de la empresa utilizando el comando ping 209.165.201.2 para verificar el alcance.



d. Utilice el comando telnet 209.165.201.2 a Telnet para la dirección IP del router de la empresa.

e. Autentique el router de la empresa con el nombre de usuario admin y la contraseña cisco123.

f. Utilice el comando mostrar usuarios para ver la conexión activa de Telnet al router de la empresa.



¿Por qué se considera Telnet un protocolo inseguro para administrar un dispositivo de manera remota?

Al igual que en el protocolo FTP la información no está encriptada esto puede ocasionar una vulnerabilidad en nuestro sistema.

Parte 4: Acceda de manera remota a un router de la empresa mediante SSH

Paso 1: Conéctese de manera remota al router de la empresa.

a. Introduzca el sitio Gotham Healthcare Branch y luego haga clic en la computadora Tim.

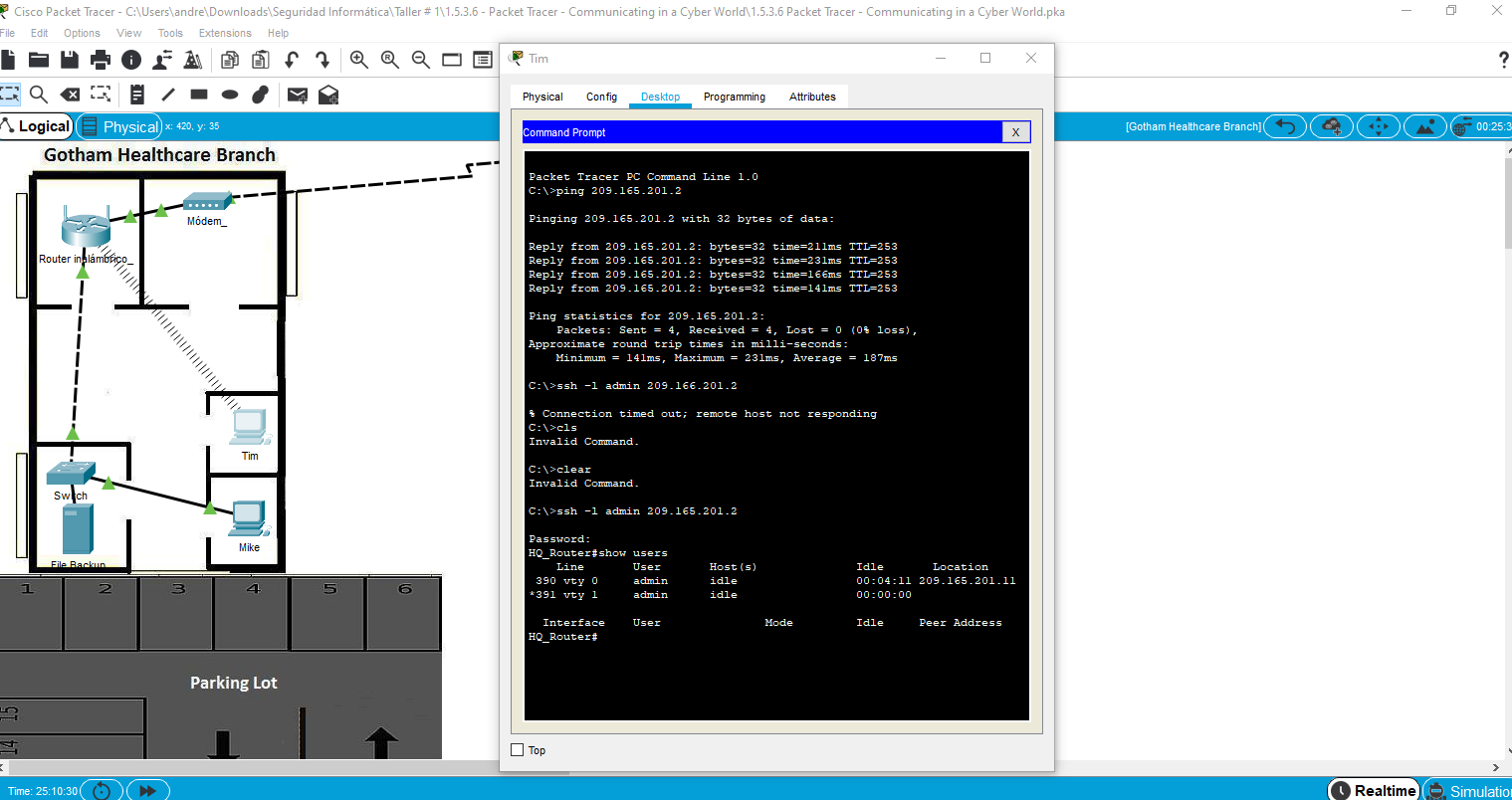
b. Haga clic en la ficha Escritorio y luego haga clic en Petición de ingreso de comando.

c. Haga ping al router de la empresa utilizando el comando ping 209.165.201.2 para verificar el alcance.

d. Utilice el comando ssh -l admin 209.165.201.2 a SSH para la dirección IP del router de la empresa.

e. Autentique el router de la empresa con la contraseña cisco123.

f. Utilice el comando mostrar usuarios para ver la conexión activa de SSH al router de la empresa.



¿Por qué se considera SSH un protocolo inseguro para administrar un dispositivo de manera remota?

Actualmente no se considera un protocolo tan inseguro debido a que la información si está encriptada a diferencia de Telnet o FTP.

Introduzca el modo de configuración global mediante el uso del comando configurar terminal. h. Cree una contraseña secreta de cisco con el comando permitir contraseña secreta de cisco.

