Protocolos de Comunicación TCP/IP

Trabajo Práctico N° 7

Temas:

- Aplicaciones TCP/IP.
- Seguridad Informática.

1. FTP y TCP.

a) Muestre el intercambio temporal de segmentos, con **todos** los campos de la cabecera de **TCP** relevantes, que se utilizan para establecer una conexión TCP entre un Cliente FTP y un Servidor FTP.

b) Idem a), asumiendo que el cliente ejecuta Comando Externo DIR. Asuma que el cliente ejecutó el Comando Interno **PASV** previo al envío del comando.
Nota: Asuma valores de parámetros que Ud. necesite (direcciones IP, Puertos efímeros, números de secuencia iniciales, etc).

2. Completar la Tabla 1 con el protocolo de capa de aplicación que usa cada comando y escribir el resumidamente el significado o acción del comando. En aquellos casos que un comando corresponda a más de un protocolo, indicar los mismos y el significado en cada uno.

Comando	Protocolo	Significado
GET		
PORT		
HELO		
STAT		
MAIL FROM		
DATA		
RETR		
RCPT TO		
LIST		
PASV		

Tabla 1: Comandos de Capa de Aplicación.

3. Protocolo HTTP-TCP

Un explorador de internet se conectará a través de HTTP 1.1 con pipelining para bajar una página web compuesta de dos imágenes: IMG1 e IMG2. El tamaño de la respuesta HTTP que contiene el archivo html que describe la página web es de 2000 Bytes y el que contiene las imágenes es de 6000 Bytes (cada imagen). El tamaño de las peticiones HTTP son de

200 Bytes. El tamaño de la ventana de recepción en ambos extremos son de 6000 Bytes y el MSS de la conexión es de 1000 Bytes.
En base a estos datos, muestre el intercambio de mensajes TCP y HTTP entre el explorador y el servidor HTTP. En los segmentos TCP, no muestre los SN y AN, sino solamente los flags relevantes.
Debe mostrar el establecimiento de la conexión y asumir que en el tercer segmento del inicio de conexión se pueden enviar datos, como en realidad sucede en TCP.
En la implementación de TCP se hace uso de ACK Retardados (Delay ACK) y también de técnicas de control de congestión, es decir arranque lento ("slow start") y evitación de la congestión ("congestion avoidance").
Nota: Asuma que ningún segmento TCP transmitido llega con error o es descartado.

4. FTP

Un cliente FTP se encuentra ubicado en una red privada, según muestra la Figura 1. La conexión de dicha red a internet es a través de un router que implementa NAT y PAT. Muestre según formato de la Tabla 2. el intercambio de segmentos TCP, cuando los mismos ingresan y egresan del router (en ambas direcciones), para los siguientes casos:

a) Establecimiento de la conexión entre el cliente FTP y el Servidor FTP.

b) Cliente ejecuta el comando ls. Mostrar los comandos FTP que se ejecutan y el primer segmento transmitido (entre ambos sistemas finales) para el establecimiento de la conexión para la transferencia de datos. Asuma que FTP trabaja en su forma por defecto y que el router posee todos sus puertos abiertos.

NOTA: Asuma ud. los puertos efímeros que necesite.

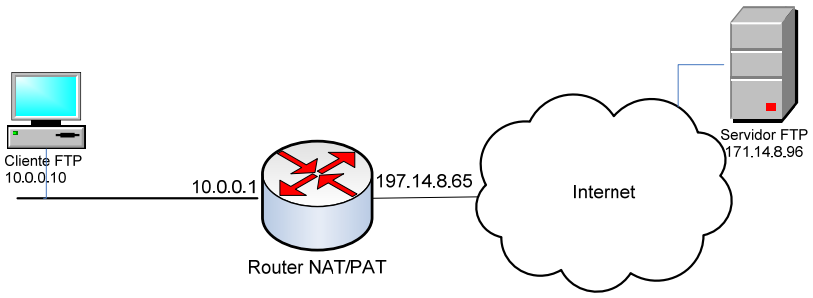
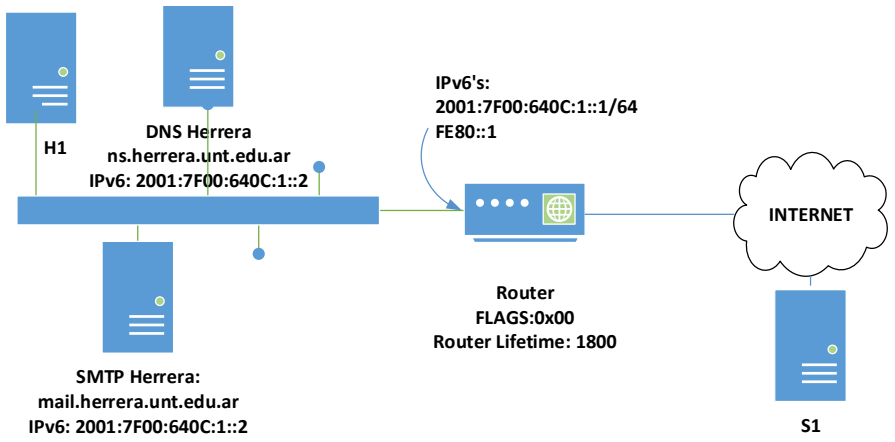


Figura 1: Escenario para problema de FTP

Desde - Hacia	Flags TCP	Port Origen	Port Destino	Comando ftp	Observaciones
Cliente - Router	…	…	…		
Router - Serv.	…	…	…		

Tabla 2: Formato tabla para Segmentos TCP.

5. Aplicaciones – SMTP/POP3



a) Se envía un correo desde una computadora H1 con la cuenta remitente ssaade@herrera.unt.edu.ar al destino: fhlutz@gmail.com. Indique el paso a paso a nivel de capa de **aplicación** desde la escritura del correo hasta que el usuario destino recoge dicho email. Debe detallar los protocolos, dirección del flujo de información, servidores y aplicaciones que intervienen, etc. Asuma cliente POP3.

b) Indique la configuración de H1 para el envío y recepción de correos electronicos, asumiendo que el servidor SMTP de Herrera actúa como servidor POP3.

6. Realice una tabla que relacione los tipos de ataques y los servicios de seguridad que podrían dar solución a esos ataques.

7. Mencione al menos tres servicios de seguridad que puede proveer la criptografía de clave pública y muestre como pueden ser implementados.

8. Muestre con un diagrama usando criptografía de clave pública como se implementa conjuntamente los servicios de autenticidad y confidencialidad en una transmisión entre un emisor y un receptor.

9. Explique los pasos del proceso de creación de certificado de clave pública y como se obtiene el servicio de seguridad de No repudio con dicho certificado.