Examen de Introducción a las Redes de Computadoras y Comunicación de Datos
(ref: eirc0603.doc)
24 de febrero de 2006

***Atención**: para todos los ejercicios, suponga que dispone de los tipos de datos básicos (p.ej. lista, cola, archivo, string, etc.) y sus funciones asociadas (ej: tail(lista), crear(archivo), concatenar(string, string).*
Se debe considerar la presentación del examen, cuidando que la letra sea legible.

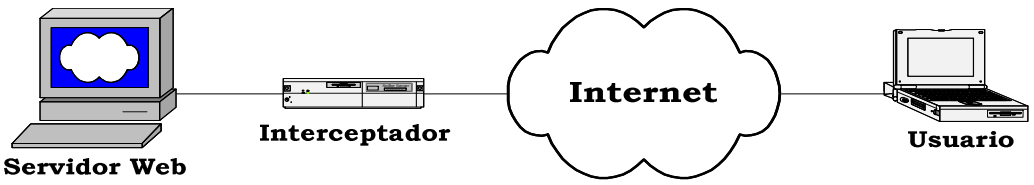
Ejercicio 1

Un ataque de "*SYN-flooding*" contra un servidor consiste en inundarlo de solicitudes de conexión TCP con direcciones IP origen falsas y/o inalcanzables. Ello determina que las conexiones TCP no se establezcan ocasionando en el servidor una reserva de recursos que no se utilizarán que puede terminar en un *Denial of Service* (*DoS*). Éstas conexiones que no terminan de establecerse son conocidas como "embrionarias".

Se pretende instalar delante de un Servidor Web un hardware específico destinado a protegerlo del ataque mencionado "*SYN-flooding*" buscando interceptar las solicitudes de conexiones TCP provenientes de potenciales usuarios del servidor. En caso de ser conexiones válidas (o sea, que se establecen), el "interceptador" establecerá una conexión TCP con el servidor Web por cada una de ellas y las "conectará" internamente entre sí.

Se deben respetar las siguientes hipótesis de trabajo:

- El Servidor Web se encuentra operativo desde hace varios meses, y no se desea modificar.
- Tanto para los usuarios del Servidor Web como para los administradores del mismo, la puesta en marcha del "*interceptador*" no debe ser detectable.
- Los administradores del Servidor Web mantienen una estadística de las direcciones IP y números de puerto desde las que se conectan a él y pretenden seguir manteniéndola sin ninguna implementación adicional.
- El "*interceptador*" es una solución (hardware y software) optimizada para poder mantener un muy alto número (no infinito) de conexiones TCP hacia los usuarios y hacia el servidor.



Describa detalladamente y sin implementar:

a) todos los aspectos a tener en cuenta en el momento del diseño del "*interceptador*" para que éste opere correctamente, debiéndose conocer en todo momento la identificación exacta de cada conexión TCP. Considere todas las etapas involucradas en el uso del servidor: establecimiento, uso y liberación de cada conexión.
b) una solución que permita al "interceptador" proteger dinámicamente al Servidor Web de posibles ataques de "*SYN-flooding*".

Ejercicio 2

Se dispone de una aplicación que desea aprovechar al máximo el envío de paquetes en la red, intentando enviar paquetes del mayor tamaño posible hacia otro equipo.
Con este fin se desea implementar un proceso PMTU (*Path MTU)*, que determine el máximo MTU desde el equipo en que se ejecuta hasta un destino (dirección IP) que se le pasa como parámetro.

Se deben considerar las siguientes hipótesis:

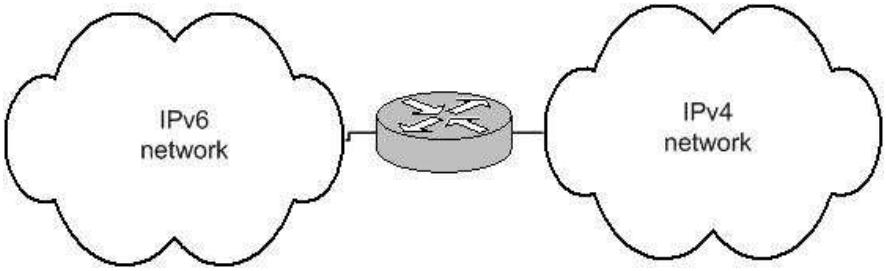
- Existe una flag en IP que habilita/deshabilita la fragmentación de paquetes en la red.
- Al recibir un router un paquete cuyo tamaño excede la MTU permitida para la interfaz de salida a utilizar, y que tiene deshabilitada la fragmentación, él mismo contesta un mensaje de notificación ICMP, indicando que requiere fragmentación.
- La interfaz que lo conecta el equipo a la red tiene una MTU definida.

Se pide:

a) Indicar como implementar un protocolo que determine el Path MTU. Especifique claramente el formato de los paquetes utilizados, y requerimientos para el funcionamiento del protocolo.
b) Especificar el mismo, en un lenguaje de alto nivel

Ejercicio 3

Sea una red sobre el protocolo IPv4 y otra red sobre IPv6, las que se encuentran interconectadas con un router. Todos los equipos de las redes cuentan en su stack de protocolos, únicamente con el protocolo de capa 3 correspondiente a la red en que se encuentran (los de la red IPv6 tiene solamente la capa red IPv6, y los de la red IPv4 tiene capa red IPv4).



Se desea lograr la interconexión entre ambas redes. Para la conversión de direcciones, se tomarán las siguientes reglas:

- IPv4 -> IPv6, se colocan 0's primeros bits, y al final la dirección IPv4
- IPv6 -> IPv4, se toman los últimos bits de la dirección y se descarta el resto.

Se pide:

a) Indicar que problemas se deben resolver, para poder interconectar las redes.
b) Escribir len un lenguaje de alto nivel as funciones que convierten datagramas en ambos sentidos:
    - **`function IPv62IPv4(d:datagrama):datagrama`**
    - **`function IPv42IPv6(d:datagrama):datagrama`**
c) ¿Como se procesaría un datagrama que se encuentra fragmentado? Indique que modificaciones debería realizar en sus funciones.