Este examen es únicamente para aquellos alumnos que no eligieron la modalidad de entrega de informes. Este examen consta de 4 ejercicios con un total de 10 puntos.

Apellidos: _____ Nombre: _____ Grupo: _____

1. (2p) ¿Cuál es la función principal del programa `netstat`?
   - ☐ **a)** Manipular las tablas de enrutamiento IP, tanto unicast como multicast.
   - ■ **b)** Listar los sockets de la máquina propia (conectados o no).
   - ☐ **c)** Listar los sockets del host cuya dirección IP se indica como parámetro.
   - ☐ **d)** Todas las anteriores.

2. (2p) Algún programa está consumiendo gran parte del ancho de banda de un host ¿Qué propone para determinar cuál es?
   - ☐ **a)** Ejecuto `netstat -ltn` para ver los servidores activos en mi máquina y los puertos a los que están vinculados. Después utilizo `nmap` con la IP remota para determinar a cuál de ellos se ha conectado algún cliente.
   - ☐ **b)** Mediante `iptraf` puedo ver de qué IP procede el tráfico inusual. Después, haciendo `traceroute` a dicha IP puedo determinar el número de saltos y el puerto vinculado al programa.
   - ■ **c)** Mediante `iptraf` puedo ver a qué puerto local corresponde el tráfico responsable. Después con `netstat -p` puedo averiguar el nombre del programa y el PID del proceso.
   - ☐ **d)** Ninguna de las anteriores, no se puede determinar la causa sin un analizador de protocolos.

3. (2p) Está usted utilizando el programa `wireshark` para analizar tráfico sospechoso que se ha constatado entre el enrutador de la LAN Ethernet y un servidor de ficheros. El enrutador, el servidor y su PC están conectados a través de un concentrador. Sin embargo, `wireshark` no muestra nada que sea achacable a dicho tráfico. ¿Qué puede estar pasando?
   - ■ **a)** La interfaz de red de su PC no está en modo promiscuo, de modo que su NIC descarta ese tráfico.
   - ☐ **b)** El host remoto malicioso está enviando tráfico IP directamente a la MAC del servidor.
   - ☐ **c)** El concentrador está enviando el tráfico Ethernet únicamente entre los puertos del enrutador y el servidor, de modo que usted no puede verlo.
   - ☐ **d)** Ninguna de las anteriores. No es posible ver tráfico ajeno en una red Ethernet en ningún caso, puesto que es un medio de difusión.

4. (4p) Explica cuáles son los fundamentos teóricos y prácticos en los que se basa el funcionamiento del programa `traceroute`.