Ejercicios de repaso y autoevaluación

1. Complete la siguiente oración:

Se define el término "red" como un conjunto de dispositivos físicos (_HARDWARE_) y de programas (_SOFTWARE_) mediante el cual se comunican los ORDENADORES autónomos para compartir información. Cada uno de los ordenadores conectados a la red se denominan "CLIENTES/NODOS

2. Busque en la sopa de letras cinco medios de comunicación de un sistema de comunicación. Tenga en cuenta que los nombres de los medios pueden estar en español o en inglés:

A	B	E	R	Z	M	A	R	S	A
O	L	S	A	R	O	U	T	E	R
B	E	W	A	R	D	E	R	T	I
B	R	I	D	G	E	S	A	E	L
D	A	T	A	R	M	A	N	I	E
O	C	C	A	R	A	E	L	I	S
L	R	H	S	E	R	T	O	U	L
A	S	E	M	A	R	T	I	O	N

3. Indique a qué tipo de conector de un sistema de comunicación se corresponden las siguientes definiciones:

fibra optica

a. Tipo de cableado especial por el que los datos se transmiten a través de la luz en lugar de por corriente eléctrica.

Sistema de cableado

b. Estructura de cables que se utiliza para conectar entre sí los distintos recursos, componentes y estaciones de trabajo que forman parte de una red.

inalambrica (wifi, bluetooth)

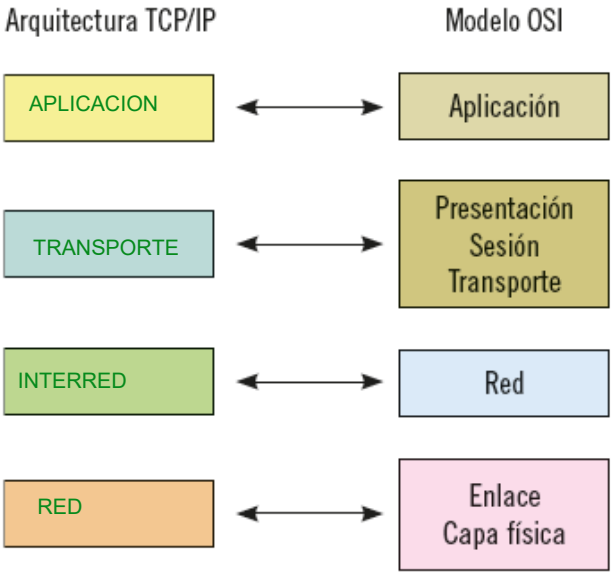
c. Enlaces que permiten la transmisión de la información a través de ondas electromagnéticas sin necesidad de tener una conexión física.

4. Rellene la siguiente tabla, indicando en la columna de la derecha las capas del modelo OSI a las que corresponden las definiciones de las celdas de la izquierda:

MODELO OSI	
NIVEL – CAPA	**DESCRIPCIÓN**
APLICACIÓN	Ofrece a las aplicaciones la posibilidad de acceder a los servicios de red para realizar el trabajo encomendado.
ENLACE DE DATOS	Divide el flujo de bits en unidades con formato mediante el uso de protocolos (puentes *-bridges-)*.
Transporte RED	Asegura la correcta recepción de la información. Establece las comunicaciones y determina la ruta de los datos en la red (enrutador *-router-)*.
FÍSICO	Se ocupa de transmitir el flujo de bits a través del medio (cables, tarjetas y repetidores).
SESIÓN	Establece, mantiene y finaliza la comunicación entre las aplicaciones en el momento apropiado.
PRESENTACIÓN	Convierte las distintas representaciones de datos para que puedan ser entendibles por el usuario.

5. Rellene los recuadros de las capas de la arquitectura TCP/IP que se corresponden con las capas del modelo OSI situado a la derecha:

Correspondencia de capas entre modelos TCP/IP y OSI



6. ¿Cuál de los siguientes servicios no está incorporado a cada capa del modelo TCP/ IP?

a. Direccionamiento.
b. Control de la reparación de datos.
c. Fragmentación.
d. Nomenclatura.

7. Relacione las siguientes características de las direcciones IP del protocolo IPv4 con las clases de direcciones mencionadas a continuación:

a. Los 24 primeros bits corresponden a la identificación de la red y los otros 8 a la identificación del equipo.
b. Direcciones IP reservadas para su uso en investigación.
c. Los 16 primeros bits (2 *bytes)* identifican la red y los otros 16 al equipo.
d. Los 8 primeros bits (que es lo mismo que 1 *byte)* identifican la red y los 24 restantes (3 *bytes)* identifican al equipo de la red.
e. Direcciones IP que envían la información a varias interfaces distintas.

D Clase A.
C Clase B.
A Clase C.
E Clase D.
B Clase E.

8. Dentro del protocolo IPv4, indique a qué concepto se refieren las siguientes definiciones:

Direccion de red

Puerta enlace

Broadcast

loopback

a. Dirección que tiene los bits de host iguales a cero. Sirve para definir la red en la que se ubica.
b. Es la dirección del *router* de la red y puede tomar cualquiera de las direcciones de un rango.
c. Dirección que sirve para enviar un paquete a todos los *hosts* de una red. Esta dirección tiene los bits correspondientes a *host* iguales a 255.
d. Son direcciones "127.x.x.x" que se reservan para designar la propia máquina. Se suelen utilizar para comprobar las propias interfaces de red.

9. ¿Cuál de los siguientes comportamientos irregulares de una red no se detecta con el análisis de resultados facilitado por el proceso de monitorización de la misma?

a. Tráfico inusual de la red.
b. Elementos principales de la red.
c. Utilización motivada de la red.
d. Calidad del servicio.

10. ¿Qué es un *sniffer*? ¿En qué protocolo se utiliza?

es un programa o dispositivo que captura toda la informacion que circula por una red, y los envia a todos los integrantes de la misma, siendo estos los que aceptan o no la informacion que les llega, se utiliza en la capa de transporte y protocolo Ethernet

11. De entre las siguientes herramientas, hay una que no se corresponde con un *sniffer*. ¿Cuál es?

a. Ettercap.
b. Hobbit-Xymon.
c. Wireshark.
d. Kismet.

12. Complete la siguiente oración:

El funcionamiento de la herramienta hobbit-Xymon se basa en el envío periódico de peticiones y el correspondiente registro de la respuesta recibida. Si recibe un valor que no está en el rango esperado envía una alerta al administrador mediante un correo electrónico

13. Mencione tres actividades para las cuales las herramientas SIM son especialmente útiles:

son herramientas de analisis del trafico de una red y son especialmente útiles en analisis de la seguridad a posteriori, detectando identificando y reportando eventos de seguridad, pronosticando y previeiendo amenazas y monitorizando ataques en tiempo real entre otras funciones

14. ¿Cuál de las siguientes opciones no se corresponde con algún beneficio que aporta la utilización de un SEM?

a. Activación de alertas programadas.
b. Acceso a los registros mediante una interfaz central inconsistente.
c. Gestión de eventos de varios sistemas operativos con un solo SEM.
d. Representación gráfica de la actividad.

15. Rellene la siguiente tabla, indicando las distintas características, funciones y limitaciones de un cortafuegos o *firewall*.

CORTAFUEGOS O *FIREWALL*
Características
- Control de servicios - Control de direcciones - Control de usuarios - Control de comportamiento
Funciones
Mantener a usuarios no autorizados fuera de la red No permite salida y/o entrada de servicios potencialmente peligrosos Protege contra ciertos ataques de suplantacion de ip Simplifica la admón de la red dejando solo un puerto de engtrada abierto permite configurar donde realizar la supervision y auditoria de eventos de seguridad
Limitaciones
- no protege contra amenazas internas - ni contra lo que no pasa por el puerto del cortafuegos - puede proporcionar una falsa sensación de seguridad, y realmente se necesitan mas elementos, como antivirus antimalwares, etc para tener un nivel de seguridad aceptable