



Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Enero de 2013

Apellidos, Nombre: _____

Cuestión 1.- Referente a las VPN (1 punto)

- (a) Comente brevemente que aporta una VPN en el ámbito de la seguridad informática.
- (b) El término IPSec hace referencia a ...
- (c) Justifique si tiene sentido o no el uso de una VPN en una red local de una pequeña oficina.

Cuestión 2.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo como sigue: (1 punto)

- (a) Ataques a la confidencialidad.
- (b) Ataques a la autenticidad.
- (c) Ataques a la disponibilidad.
- (d) Ataques a la integridad.

Describa brevemente cada uno de ellos y ponga un ejemplo de este tipo de ataques.

Cuestión 3.- Marque las afirmaciones correctas: (1 punto)

- Un Firewall de filtrado de paquetes trabaja en el nivel de aplicación del modelo OSI.
- Un Firewall de filtrado de paquetes trabaja en el nivel de red del modelo OSI.
- Un Proxy trabaja en el nivel de aplicación del modelo OSI.
- Un Proxy trabaja en el nivel de red del modelo OSI.

Cuestión 4.- Referente a la las infraestructuras de clave pública PKI responda a las siguientes cuestiones: (1 punto)

- (a) ¿Para que sirven la autoridades de certificación en una infraestructura PKI?
- (b) ¿Cual es la diferencia entre una clave publica o privada, y un certificado digital?
- (c) ¿Que relación tiene el protocolo SSL con un certificado digital?

Cuestión 5.- Enumere y describa brevemente al menos 3 métricas usadas habitualmente en la calidad de servicio para redes IP. (1 punto)

Cuestión 6.- En el ámbito de QoS tratado en la asignatura, en el *jitter* influye: (0.5 puntos)

- El tamaño de cola de los enrutadores.
- La velocidad del enlace.
- El retraso de transmisión.

Cuestión 7.- En el ámbito de QoS tratado en la asignatura, el uso de un buffer mejora la calidad de servicio de los siguientes tipos de aplicaciones IP: (0.5 puntos)

- Aplicaciones dedicadas a VOIP.
- Aplicaciones de vídeo bajo demanda.
- Juegos interactivos.
- Servidores de contenidos Web.

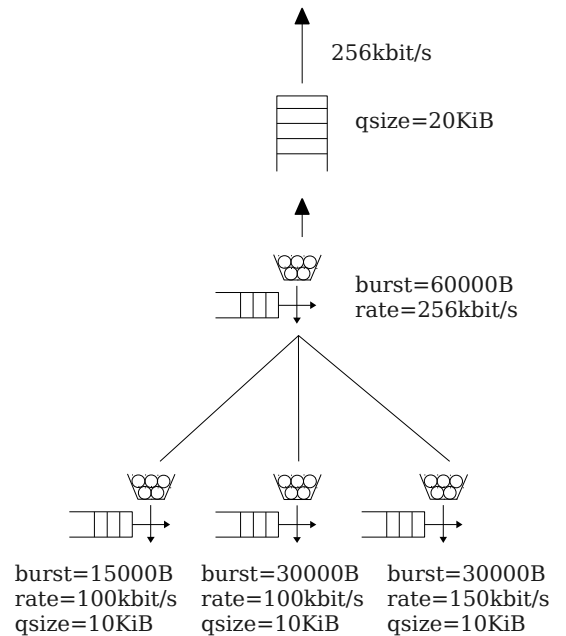
Cuestión 8.- Indique los principales motivos por los que DIFFSERV ha tenido mayor aceptación que INTERSERV. (1 punto)

Cuestión 9.- Para un enlace de 10Mbit/s se utiliza una disciplina de planificación WFQ que utiliza tres colas de mismo tamaño. (1.5 puntos)

- (a) Se quiere garantizar un caudal 6Mbit/s y una latencia de 50ms para la cola 1. Configure correctamente los quatoms y el tamaño de cola suponiendo una MTU de 1500Bytes.
- (b) Estime el jitter para cada una de las colas.

Cuestión 10.- Dada la configuración de cubetas de las figura: (1.5 puntos)

- (a) Indique los posibles errores o problemas existentes con la configuración establecida.
- (b) En la cola de la izquierda operará un servicio interactivo que envía 10 paquetes/s. Configure correctamente los parámetros de todas las cubetas para que el servicio interactivo tenga máxima calidad de servicio.
- (c) ¿Como influye el tamaño de los paquetes del servicio interactivo en la configuración del apartado anterior?





Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Febrero de 2013

Apellidos, Nombre: _____



Cuestión 1.- Describa brevemente las similitudes y las diferencias entre un Proxy y un Firewall. (1 punto)

Cuestión 2.- En las clases de problemas de la asignatura se realizaron escaneos de puertos utilizando la herramienta NMAP, describa brevemente en que consiste un escaneo de puertos. (1 punto)

Cuestión 3.- Señale las afirmaciones correctas: (0.5 puntos)

- Un Firewall protegen de los ataques realizados proveniente de la red interna.
- Un Firewall protege de ataques de ingeniería social.
- Un Firewall protege de virus informáticos.
- Protege de ataques procedentes de la red exterior.

Cuestión 4.- Describa brevemente la diferencia entre un Proxy HTTP directo y un Proxy HTTP inverso. (1 punto)

Cuestión 5.- Describa brevemente en que consiste un túnel de red en el ámbito de la asignatura y para que ha sido utilizado. (1 punto)

Cuestión 6.- Indique las principales diferencias entre el cifrado simétrico y el asimétrico. (1 punto)

Cuestión 7.- ¿En que consiste el Jitter? Proponga y defina alguna forma de medirlo. (1 punto)

Cuestión 8.- Para cada tipo de aplicación, indique cual es la métrica, de las estudiadas en la asignatura, que más afecta a la calidad de dicho servicio: (1 punto)

(a) VOIP: _____

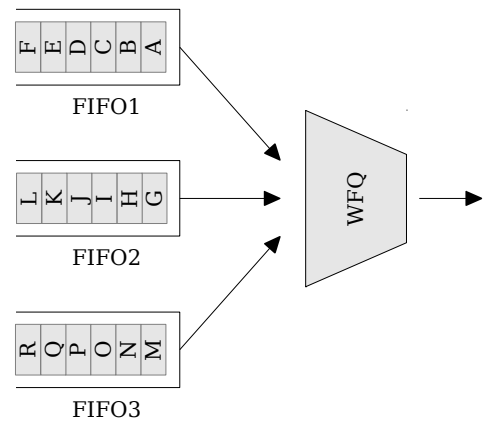
(b) Vídeo bajo demanda: _____

(c) IPTV: _____

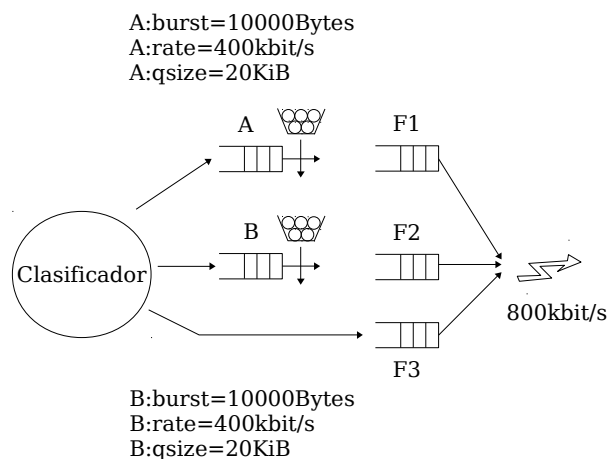
(d) Aplicaciones interactivas: _____

Cuestión 9.- Dado el esquema de la figura y aplicando el algoritmo WFQ indique el orden en el que salen los paquetes en las siguientes condiciones: (1 punto)

- (a) Comenzando por la FIFO1 y con quantum: $q_1=3$, $q_2=1$ y $q_3=1$.
- (b) Si el enlace de salida es de 1.5Mpaq/s calcule el tamaño de cada cola para que el tiempo de espera máximo sea inferior a 70ms usando los quantum anteriores.



Cuestión 10.- El esquema de la figura representa la configuración de control de tráfico de un router. A y B son cubetas con fichas y FX son colas de prioridad (F1 es la más prioritaria). (1.5 puntos)



- (a) En el esquema se establece una configuración para las cubetas. Dada esa configuración ¿las tres clases de servicio tienen un caudal garantizado? Justifique adecuadamente su respuesta.
- (b) Se propone cambiar la configuración de la cubeta A: $rate=256Kbit/s$. Permaneciendo el resto de parámetros inalterado, calcule el tamaño de la cola F1 para que el tiempo total de espera de los paquetes clasificados en la cola A sea inferior a 1s.
- (c) Si la cola F2 tiene un tamaño de 50KiB y la cola F1 el tamaño calculado en el apartado (b), calcule Jitter para esta clase de servicio.



Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Septiembre de 2013

Apellidos, Nombre: _____



Cuestión 1.- Describa brevemente las similitudes y las diferencias entre un Proxy y un Firewall. (1 punto)

Cuestión 2.- Describa brevemente la diferencia entre un Proxy HTTP directo y un Proxy HTTP inverso. (1 punto)

Cuestión 3.- En el ámbito de la asignatura describa lo que aportan los protocolos SSL y TLS. ¿Cual es la diferencia entre ambos?. (1 punto)

Cuestión 4.- Describa brevemente el cometido de las autoridades de certificación en una infraestructura PKI. (1 punto)

Cuestión 5.- ¿En que consiste el Jitter? Proponga y defina alguna forma de medirlo. (1 punto)

Cuestión 6.- Describa brevemente las tecnologías DIFSERV e INTERSEV (1 punto)

Cuestión 7.- Describa brevemente los métodos de regulación de velocidad llamados Cubeta con pérdidas y Cubeta con fichas. ¿Cuales son las diferencias y similitudes entre ambos? (1 punto)

Cuestión 8.- Un router está sirviendo tres clases de servicios clasificando cada clase una cola FIFO de 100 paquetes. El router utiliza WFQ con igual quantum para extraer paquetes de las colas y el enlace de salida tiene una caudal de 640Kbit/s. (1.5 puntos)

- (a) ¿Cual es el caudal mínimo garantizado para cada clase de servicio?
- (b) Calcule el retraso máximo si el tamaño máximo de los paquetes es 100Bytes incluyendo el retraso de transmisión.

Cuestión 9.- Una corporación tiene una sede remota y ha contratado un SLA a un ISP que garantiza un caudal de 5Mbit/s. Se desea realizar una configuración con diferentes políticas para garantizar el funcionamiento de varios servicios con ciertas restricciones asegurando los siguientes servicios prioritarios: (1.5 puntos)

- Una aplicación interactiva de acceso a base de datos remota que realiza consultas esporádicas pero limitadas a 500KiB.
- 10 canales de para VOIP cuyo codec necesita 150kbit/s.

- (a) Proponga un esquema con diversas disciplinas para dar servicio justificándolo.
- (b) ¿Cual es el tiempo de respuesta de la aplicación interactiva?
- (c) Que ancho de banda queda disponible para el resto de conexiones.



Grado en Ingeniería Informática - Tecnologías de la Información
Tecnologías Avanzadas de la Información - 3ª Conv. Diciembre 2013

Apellidos, Nombre: _____



Cuestión 1.- Describa brevemente las similitudes y las diferencias entre un Proxy y un Firewall. (1 punto)

Cuestión 2.- En las clases de problemas de la asignatura se realizaron escaneos de puertos utilizando la herramienta NMAP, describa brevemente en que consiste un escaneo de puertos. (1 punto)

Cuestión 3.- Señale las afirmaciones correctas: (0.5 puntos)

- Un Firewall protegen de los ataques realizados proveniente de la red interna.
- Un Firewall protege de ataques de ingeniería social.
- Un Firewall protege de virus informáticos.
- Protege de ataques procedentes de la red exterior.

Cuestión 4.- Describa brevemente la diferencia entre un Proxy HTTP directo y un Proxy HTTP inverso. (1 punto)

Cuestión 5.- Describa brevemente en que consiste un túnel de red en el ámbito de la asignatura y para que ha sido utilizado. (1 punto)

Cuestión 6.- Indique las principales diferencias entre el cifrado simétrico y el asimétrico. (1 punto)

Cuestión 7.- ¿En que consiste el Jitter? Proponga y defina alguna forma de medirlo. (1 punto)

Cuestión 8.- Para cada tipo de aplicación, indique cual es la métrica, de las estudiadas en la asignatura, que más afecta a la calidad de dicho servicio: (1 punto)

(a) VOIP: _____

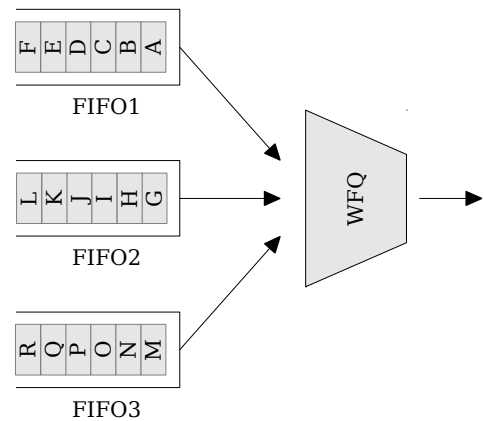
(b) Vídeo bajo demanda: _____

(c) IPTV: _____

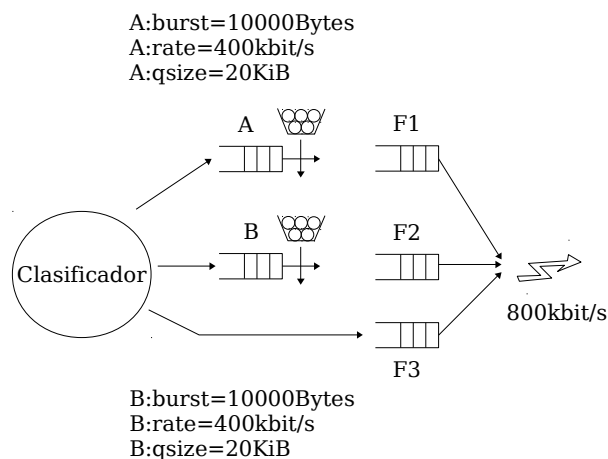
(d) Aplicaciones interactivas: _____

Cuestión 9.- Dado el esquema de la figura y aplicando el algoritmo WFQ indique el orden en el que salen los paquetes en las siguientes condiciones: (1 punto)

- (a) Comenzando por la FIFO1 y con quantum: $q_1=3$, $q_2=1$ y $q_3=1$.
- (b) Si el enlace de salida es de 1.5Mpaq/s calcule el tamaño de cada cola para que el tiempo de espera máximo sea inferior a 70ms usando los quantum anteriores.



Cuestión 10.- El esquema de la figura representa la configuración de control de tráfico de un router. A y B son cubetas con fichas y FX son colas de prioridad (F1 es la más prioritaria). (1.5 puntos)



- (a) En el esquema se establece una configuración para las cubetas. Dada esa configuración ¿las tres clases de servicio tienen un caudal garantizado? Justifique adecuadamente su respuesta.
- (b) Se propone cambiar la configuración de la cubeta A:rate=256Kbit/s. Permaneciendo el resto de parámetros inalterado, calcule el tamaño de la cola F1 para que el tiempo total de espera de los paquetes clasificados en la cola A sea inferior a 1s.
- (c) Si la cola F2 tiene un tamaño de 50KiB y la cola F1 el tamaño calculado en el apartado (b), calcule Jitter para esta clase de servicio.



Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Enero de 2014

Apellidos, Nombre: _____



Cuestión 1.- En el ámbito de la seguridad informática defina brevemente los siguientes conceptos/términos: seguridad lógica, seguridad física, análisis de riesgo, VPN e IPSec. *(1 punto)*

Cuestión 2.- La ingeniería social es el origen de la mayoría de los ataques informáticos. Describa brevemente en que consiste e indique cual es la única contramedida efectiva. *(1 punto)*

Cuestión 3.- Indique las ventajas y los inconvenientes de utilizar un Proxy frente a un Firewall de filtrado de paquetes en el ámbito de la seguridad informática. *(1 punto)*

Cuestión 4.- ¿Qué son las funciones HASH y qué utilidad tienen en el ámbito de la seguridad informática? *(0.5 puntos)*

Cuestión 5.- Describa brevemente en que consiste un túnel de red en el ámbito de la asignatura y para que ha sido utilizado. *(0.5 puntos)*

Cuestión 6.- En la asignatura se ha estudiado el cifrado simétrico y asimétrico. Indique cual se considera más seguro y justifique su respuesta. *(1 punto)*

Cuestión 7.- También se han estudiado PKIs centralizados y distribuidos, indique un ejemplo de cada uno de ellos y las principales diferencias existentes entre ambos. *(1 punto)*

Cuestión 8.- Defina los siguientes conceptos: Jitter, capacidad de ruta y capacidad de transporte. *(1 punto)*

Cuestión 9.- Indique las métricas QoS estudiadas que más afectan a: (1) Aplicaciones interactivas (2) servicios de streaming. *(0.5 puntos)*

Cuestión 10.- Un router está sirviendo 4 clases de servicios clasificando cada clase una cola FIFO de 150 paquetes. El router está configurado con una política WFQ con igual quantum para extraer paquetes de las colas y el enlace de salida tiene una caudal de 1200Kbit/s. *(1.5 puntos)*

- (a) ¿Cuál es el caudal mínimo garantizado para cada clase de servicio?
- (b) Calcule el retraso máximo si el tamaño máximo de los paquetes es 1492Bytes.
- (c) El retraso de la red del ISP es de 80ms, indique las modificaciones necesarias en la configuración del sistema para poder utilizar VOIP en sólo una de las clases de servicio. Proponga una solución concreta.

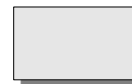
Cuestión 11.- Se dispone de una cubeta con fichas con una cola de 200KiB, con una cubeta de 50KiB y una velocidad de entrada de fichas de 100KiB/s. Midiendo el jitter como variación máxima del retraso de dos paquetes consecutivos: *(1 punto)*

- (a) Calcule el jitter producido por la cubeta.
- (b) Calcule el jitter suponiendo que al estar tras un clasificador, la cubeta es usada exclusivamente por un flujo que envía ráfagas de 80KiB cada 2 segundos.



Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Febrero de 2014

Apellidos, Nombre: _____



Cuestión 1.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo como en cuatro grandes grupos: ataques a la confidencialidad, ataques a la autenticidad, ataques a la disponibilidad y ataques a la integridad. Describa brevemente cada uno de ellos mediante un ejemplo.

(1 punto)

Cuestión 2.- Referente a los ataques informáticos:

(1 punto)

- (a) Indique en que consiste el Spoofing.
- (b) Describa cada uno de estos ataques: IP Spoofing, DNS spoofing, Web Spoofing, ARP Spoofing.
- (c) Ordénelos justificando el orden e indicando cuales son considerados más peligrosos suponiendo que puede ocurrir en el interior una red local de una organización.

Cuestión 3.- Describa brevemente las diferencias entre un Proxy HTTP directo y un Proxy HTTP inverso.

(0.5 puntos)

Cuestión 4.- ¿Cual es el cometido de las autoridades de certificación en una infraestructura PKI?

(0.5 puntos)

Cuestión 5.- En la asignatura se ha estudiado el cifrado simétrico y asimétrico. Indique cual se considera más seguro y justifique su respuesta.

(1 punto)

Cuestión 6.- En los sistemas informáticos no se almacenan las contraseñas de los usuarios en claro, se almacena el resultado de la función HASH aplicada a la contraseña. ¿Por qué a pesar de esta medida de seguridad se obliga a los usuarios a usar contraseñas con: más de 6 caracteres, al menos con un número, al menos una letra mayúscula y un carácter especial?

(1 punto)

Cuestión 7.- Para las siguientes aplicaciones indique cuales son las métrica QoS que considere más relevantes justificando su respuesta:

(1 punto)

- (a) Aplicaciones VOIP.
- (b) Aplicaciones de vídeo bajo demanda.
- (c) Servicios de almacenamiento en la nube.
- (d) Servidores de contenidos Web.

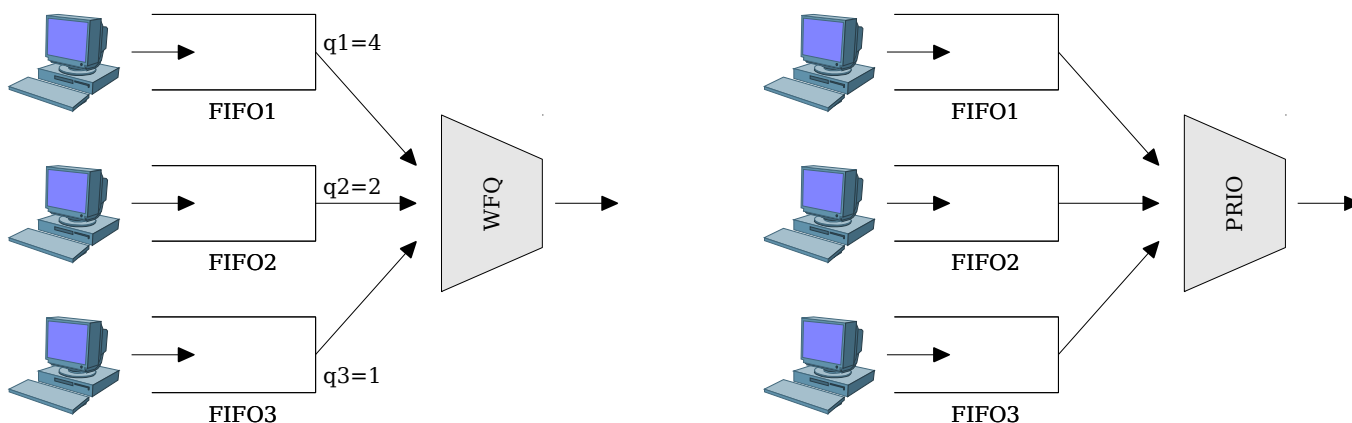
Cuestión 8.- Describa brevemente los métodos de regulación de velocidad llamados *Cubeta con pérdidas* y *Cubeta con fichas*. ¿Cuales son las diferencias y similitudes entre ambos?

(1 punto)

Cuestión 9.- Las tecnologías DIFFSERV e INTERSERV, tienen un mismo objetivo común. Coméntelo brevemente e indique y las diferencias entre ambas.

(1 punto)

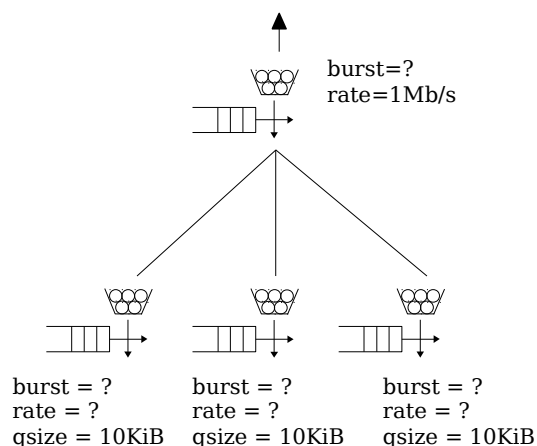
Cuestión 10.- Las figuras muestran dos configuraciones de un router, una basada en el algoritmo WFQ y otra usando colas de prioridad, siendo FIFO1 la cola más prioritaria y el enlace de salida de 10Mb/s. (1 punto)



- (a) ¿Cual es el caudal mínimo garantizado para cada uno de los equipos?
- (b) Calcule en ambos casos el tamaño máximo de la cola FIFO1 para que el retraso no supere los 150ms.

Cuestión 11.- Dada la configuración de cubetas de la figura: (1 punto)

- (a) Configure los parámetros de las cubetas de la figura para que el comportamiento sea similar a WFQ de la figura anterior.
- (b) Calcule el máximo retraso para cada una de las 3 colas





Grado en Ingeniería Informática - Tecnologías de la Información

Tecnologías Avanzadas de la Información - Enero de 2015

Apellidos, Nombre: _____



Cuestión 1.- La ingeniería social es el origen de la mayoría de los ataques informáticos. Describa brevemente en que consiste e indique cual es la única contramedida efectiva. (0.5 puntos)

Cuestión 2.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo, indique cuál es la clasificación propuesta y ponga un ejemplo de cada tipo de ataque. (1 punto)

Cuestión 3.- Señale las afirmaciones correctas: (1 punto)

- Un firewall de filtrado de paquetes protege de los ataques provenientes de la red interna.
- Un proxy protege de ataques de ingeniería social.
- Un firewall de filtrado de paquetes opera con menos recursos que un proxy.
- Un proxy se puede utilizar para realizar operaciones de filtrado en el nivel de aplicación.

Cuestión 4.- Referente a los ataques informáticos: (1 punto)

- (a) Indique en que consiste el Spoofing.
- (b) Describa cada uno de estos ataques: IP Spoofing, DNS spoofing, Web Spoofing, ARP Spoofing.
- (c) Ordénelos según los considere más peligrosos, suponiendo que pueden ocurrir en el interior de una red local de una organización. Justifique el orden establecido.

Cuestión 5.- La tabla muestra la velocidad de operación del programa HASCAT en un ataque de fuerza bruta contra las diferentes funciones HASH. (1 punto)

Función	Hash/s
MD5	8511 Mh/s
SHA1	2722 Mh/s
SHA256	1120 Mh/s
SHA512	416 Mh/s
SHA-3(Keccak)	179 Mh/s
RipeMD160	1802 Mh/s
Whirlpool	65800 kh/s
LM	1374 Mh/s
NTLM	16701 Mh/s
NetNTLMv1	9066 Mh/s
NetNTLMv2	591 Mh/s

- (a) ¿Por qué se utilizan funciones HASH de contraseñas para identificar a los usuarios en los sistemas informáticos?
- (b) Basándose en los datos de la tabla ¿que función recomendaría para utilizar en un sistema informático en la nube? Justifique su respuesta.

Cuestión 6.- En la asignatura se ha estudiado el cifrado simétrico y asimétrico: (1 punto)

- (a) ¿Por qué las infraestructuras PKI estudiadas durante el curso utilizan cifrado asimétrico?
- (b) ¿Cuál es el cometido de las autoridades de certificación en la infraestructura PKI?

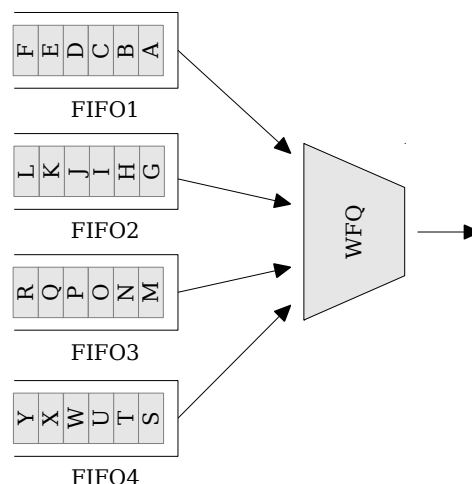
Cuestión 7.- Referente al Jitter: (1 punto)

- (a) ¿En qué consiste?
- (b) Indique los principales motivos por los que aparece el Jitter.
- (c) Proponga y defina alguna forma de medirlo.

Cuestión 8.- Indique las métricas QoS estudiadas que más afectan a: (1) Aplicaciones de vídeo conferencia (2) servicios de juegos interactivos. (0.5 puntos)

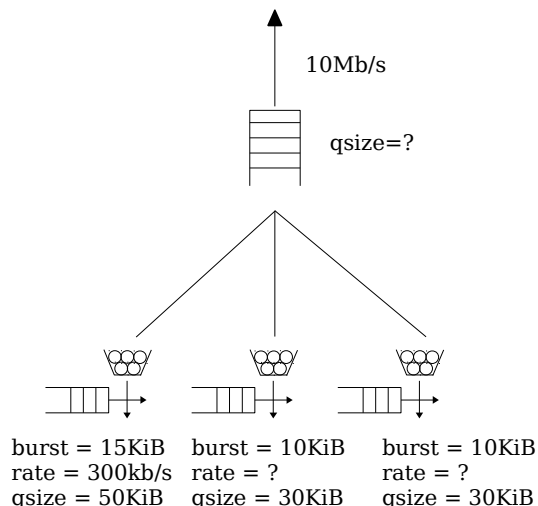
Cuestión 9.- Un router está sirviendo 4 clases de servicios, clasificando cada clase en una cola FIFO. El router está configurado con una política WFQ y el enlace de salida tiene una caudal de 1Mbit/s. (1.5 puntos)

- (a) Indique una configuración de quantums para que la FIFO1 tenga garantizado exactamente 500Kbit/s.
- (b) Con la configuración anterior indique el orden de salida de paquetes comenzando por la FIFO1.
- (c) Calcule el tamaño de la FIFO4 para que retraso máximo introducido por la cola sea inferior a 200ms.



Cuestión 10.- Dada la configuración de cubetas mostrada en la figura responda las siguientes cuestiones. (1.5 puntos)

- (a) ¿Cuál es el mínimo tamaño de la cola de salida (qsize) para que la configuración de la figura opere correctamente? Justifique la respuesta.
- (b) ¿Cuál es la restricción existente para configurar la velocidad de las cubetas (parámetro rate)? Justifique la respuesta.
- (c) Se desea utilizar la cubeta de la izquierda para servicios de vídeo conferencia. ¿Es posible, cuáles son las restricciones? Justifique la respuesta.





Grado en Ingeniería Informática - Tecnologías de la Información

Tecnologías Avanzadas de la Información - Enero de 2015

Apellidos, Nombre: _____



Cuestión 1.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo, indique cuál es la clasificación propuesta y ponga un ejemplo de cada tipo de ataque. *(1 punto)*

Cuestión 2.- Señale las afirmaciones correctas: *(1 punto)*

- Un firewall de filtrado de paquetes protege de los ataques provenientes de la red interna.
- Un proxy protege de ataques de ingeniería social.
- Un firewall de filtrado de paquetes opera con menos recursos que un proxy.
- Un proxy se puede utilizar para realizar operaciones de filtrado en el nivel de aplicación.

Cuestión 3.- Referente a los ataques informáticos: *(1 punto)*

- (a)** Indique en que consiste el Spoofing.
- (b)** Describa cada uno de estos ataques: IP Spoofing, DNS spoofing, Web Spoofing, ARP Spoofing.
- (c)** Ordénelos según los considere más peligrosos, suponiendo que pueden ocurrir en el interior de una red local de una organización. Justifique el orden establecido.

Cuestión 4.- La tabla muestra la velocidad de operación del programa HASCAT en un ataque de fuerza bruta contra las diferentes funciones HASH. *(1 punto)*

Función	Hash/s
MD5	8511 Mh/s
SHA1	2722 Mh/s
SHA256	1120 Mh/s
SHA512	416 Mh/s
SHA-3(Keccak)	179 Mh/s
RipeMD160	1802 Mh/s
Whirlpool	65800 kh/s
LM	1374 Mh/s
NTLM	16701 Mh/s
NetNTLMv1	9066 Mh/s
NetNTLMv2	591 Mh/s

- (a)** ¿Por qué se utilizan funciones HASH de contraseñas para identificar a los usuarios en los sistemas informáticos?
- (b)** Basándose en los datos de la tabla ¿que función recomendaría para utilizar en un sistema informático en la nube? Justifique su respuesta.

Cuestión 5.- Las tecnologías DIFFSERV e INTERSERV, tienen un mismo objetivo común. Coméntelo brevemente e indique y las diferencias entre ambas. *(0.5 puntos)*

Cuestión 6.- En la asignatura se ha estudiado el cifrado simétrico y asimétrico: *(1 punto)*

- (a)** ¿Por qué las infraestructuras PKI estudiadas durante el curso utilizan cifrado asimétrico?
- (b)** ¿Cuál es el cometido de las autoridades de certificación en la infraestructura PKI?

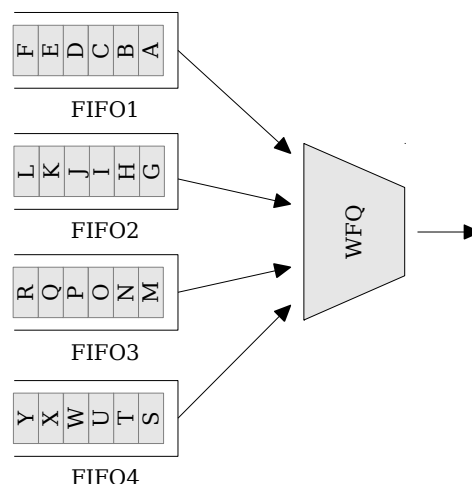
Cuestión 7.- Referente al Jitter: *(1 punto)*

- (a)** ¿En qué consiste?
- (b)** Indique los principales motivos por los que aparece el Jitter.
- (c)** Proponga y defina alguna forma de medirlo.

Cuestión 8.- Indique las métricas QoS estudiadas que más afectan a: (1) Aplicaciones de vídeo conferencia (2) servicios de juegos interactivos. *(0.5 puntos)*

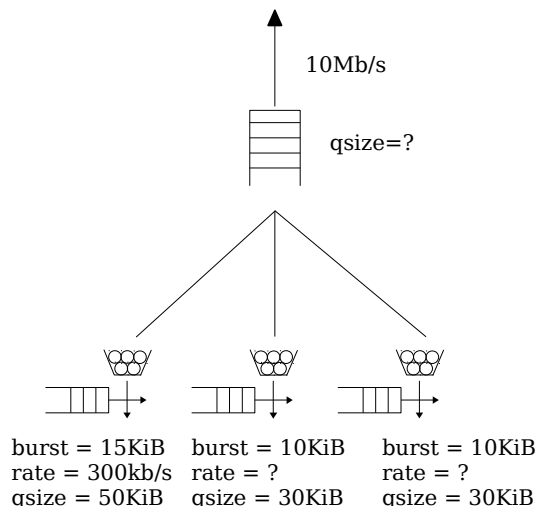
Cuestión 9.- Un router está sirviendo 4 clases de servicios clasificando cada clase en una cola FIFO. El router está configurado con una política WFQ y el enlace de salida tiene una caudal de 2Mbit/s. (1.5 puntos)

- (a) Indique una configuración de quantums para que la FIFO1 tenga garantizado exactamente 1Mbit/s.
- (b) Con la configuración anterior indique el orden de salida de paquetes comenzando por la FIFO1.
- (c) Calcule el tamaño de la FIFO4 para que retraso máximo introducido por la cola sea inferior a 150ms.



Cuestión 10.- Dada la configuración de cubetas mostrada en la figura responda las siguientes cuestiones. (1.5 puntos)

- (a) ¿Cuál es el mínimo tamaño de la cola de salida (qsize) para que la configuración de la figura opere correctamente? Justifique la respuesta.
- (b) ¿Cuál es la restricción existente para configurar la velocidad de las cubetas (parámetro rate)? Justifique la respuesta.
- (c) Se desea utilizar la cubeta de la izquierda para servicios de vídeo conferencia. ¿Es posible, cuáles son las restricciones? Justifique la respuesta.





Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Enero de 2015

Apellidos, Nombre: _____



Cuestión 1.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo. Para cada ejemplo mostrado a continuación, indique en que categoría se puede considerar: *(1.5 puntos)*

- (a) Un secuestro de sesión en un navegador Web se considera un ataque: _____
- (b) Realizar IP spoofing en una red local se considera un ataque: _____
- (c) Realizar DNS spoofing a un equipo informático se considera: _____
- (d) Saturar una red local con paquetes UDP se considera un ataque: _____
- (e) Enviar peticiones masivas HTTP desde una botnet contra un servidor WEB se considera un ataque: _____
- (f) Usar un exploit contra un navegador Web vulnerable se considera un ataque: _____

Cuestión 2.- Durante el curso se realizó la instalación de un proxy HTTP en modo inverso y en modo directo, indique brevemente: *(1 punto)*

- (a) Posibles utilidades y usos un proxy HTTP directo en una red local.
- (b) Utilidad de uno o varios proxies HTTP inversos para dar servicio HTTP.

Cuestión 3.- Se desea filtrar el tráfico P2P y el tráfico VoIP en una red local. Discuta brevemente sobre la utilización de un proxy, un firewall de filtrado de paquetes o ambos para estos escenarios: *(1 punto)*

- (a) Considere que los usuarios de la red no tienen conocimientos informáticos.
- (b) Considere que los usuarios de la red tienen conocimientos informáticos de nivel medio e intentarán saltar las restricciones.

Cuestión 4.- En la asignatura se ha dedicado un tema al estudio de las VPNs. En él se mostraban diferentes tecnologías usadas. Describa brevemente en que consiste cada una de las siguientes e indique que relación tiene con una VPN: *(1 punto)*

- (a) Túnel de red. (b) Cifrado simétrico. (c) Cifrado asimétrico. (d) IPSec.

Cuestión 5.- La tecnología DIFFSERV tiene como objetivo dotar a Internet de QoS mediante el marcado de paquetes, responda brevemente: *(1 punto)*

- (a) ¿En que consiste el marcado de paquetes?
- (b) ¿Qué tecnología diferente al marcado de paquetes usa INTERSERV y por qué fracaso?

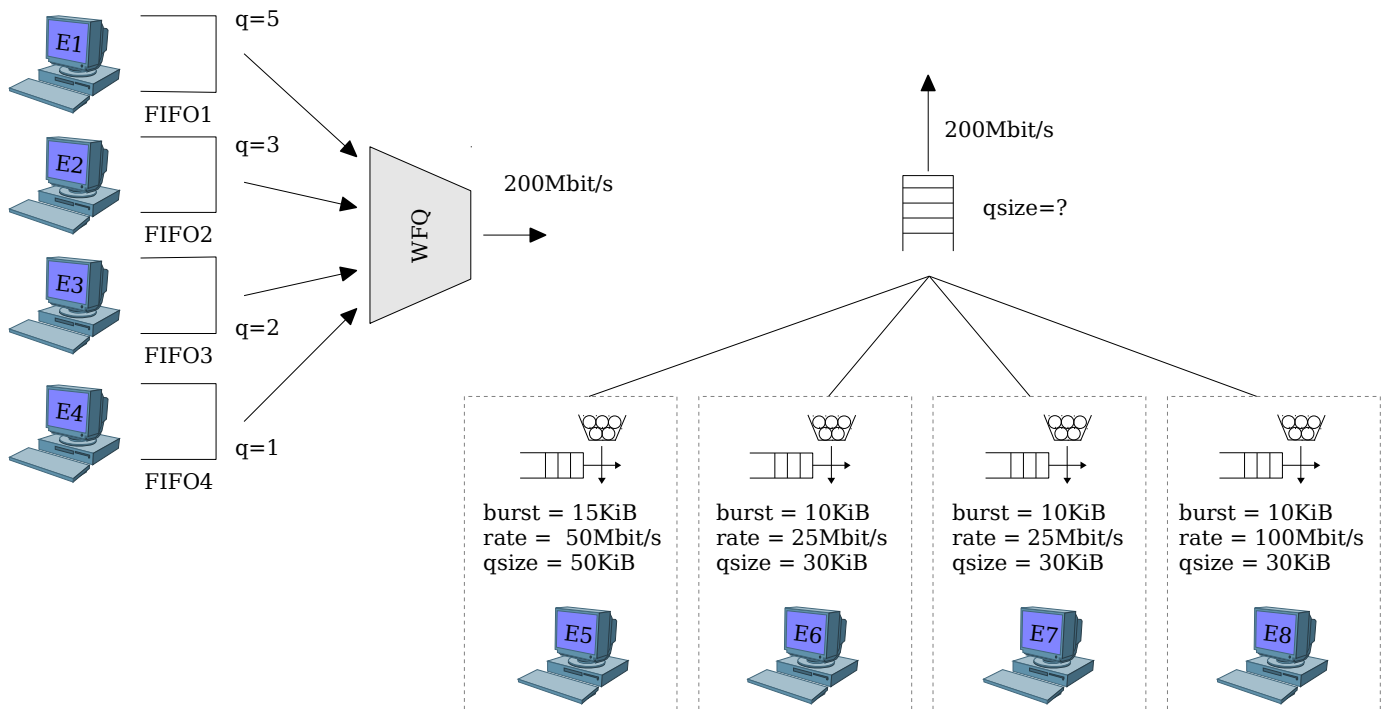
Cuestión 6.- Las infraestructuras PKI estudiadas durante el curso usan autoridades de certificación para firmar las claves públicas de terceros: *(1.5 puntos)*

- (a) ¿Cuál es el objetivo de firmar las claves públicas de terceros?
- (b) ¿Para que sirven los listados de revocación de certificados (CRLs) en una infraestructura PKI?
- (c) ¿Cual es el eslabón más débil de dicha infraestructura y que medidas adicionales se suelen tomar para aumentar la seguridad de dicho eslabón?

Cuestión 7.- Indique las métricas QoS estudiadas que más afectan a las siguientes aplicaciones concretas: (1 punto)

- (a) Skype. (b) Mario Karts on line. (c) Netflix. (d) Mensajería con WhatsApp.
 (e) Twitter (f) Gmail (g) Dropbox (h) SSH

Cuestión 8.- Dadas las dos configuraciones mostradas en la figura responda las cuestiones planteadas (2 puntos)



(a) Rellene la tabla indicando el mínimo caudal garantizado y la tasa pico usando las unidades correctas (G,M,K, etc.)

	E1	E2	E3	E4	E5	E6	E7	E8
Min. Caudal garantizado								
Tasa pico								

(b) Para la configuración WFQ rellene la tabla con el tamaño máximo de las colas para que el retraso sea inferior a 10ms. Use las unidades correctas (GiB, MiB, KiB, etc.)

	FIFO1	FIFO2	FIFO3	FIFO4
Tamaño máximo de la cola				

(c) ¿Cuál es el mínimo tamaño de la cola de salida de la estructura de cubetas (qsize) para que la configuración de la figura opere correctamente? Justifique la respuesta.

(d) Se desea utilizar la cubeta de la izquierda para servicios de vídeo conferencia. ¿Es posible, cuáles son las restricciones que hay que comprobar? Justifique la respuesta.



Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Febrero de 2016

Apellidos, Nombre: _____



Cuestión 1.- Indique cuales de los siguientes ataques **sólo** pueden ser realizados de forma directa desde el interior de una red local (justifique la respuesta). (1 punto)

- (a) IP Spoofing (b) DNS Spoofing (c) Web Spoofing
(d) ARP Spoofing (e) DoS: Flooding UDP

Cuestión 2.- Señale las afirmaciones correctas: (1 punto)

- Un firewall de filtrado de paquetes protege de los ataques provenientes de la red interna.
 Un proxy protege de ataques de ingeniería social.
 Un firewall de filtrado de paquetes opera con menos recursos que un proxy.
 Un proxy se puede utilizar para realizar operaciones de filtrado en el nivel de aplicación.

Cuestión 3.- Responda razonadamente si las siguientes afirmaciones son ciertas o falsas: (1 punto)

- (a) Un escaneo de puertos con la herramienta NMAP es considerado un tipo de ataque no estructurado.
(b) Un ataque de ingeniería social es fácilmente detectado por un sistema de detección de intrusiones IDS.
(c) Wireshark es una herramienta para realizar ataques de interrupción.

Cuestión 4.- Se desea filtrar el tráfico P2P y el tráfico VoIP en una red local. Discuta brevemente sobre la utilización de un proxy, un firewall de filtrado de paquetes o ambos para estos escenarios: (1 punto)

- (a) Considere que los usuarios de la red no tienen conocimientos informáticos.
(b) Considere que los usuarios de la red tienen conocimientos informáticos de nivel medio e intentarán saltar las restricciones.

Cuestión 5.- En la asignatura se ha dedicado un tema al estudio de las VPNs. En él que se mostraban diferentes tecnologías usadas. Describa brevemente en que consiste cada una de las siguientes e indique que relación tiene con una VPN: (1 punto)

- (a) Túnel de red. (b) Cifrado simétrico. (c) Cifrado asimétrico. (d) IPSec.

Cuestión 6.- En la asignatura se ha estudiado el cifrado simétrico y asimétrico: (1 punto)

- (a) ¿Por qué las infraestructuras PKI estudiadas durante el curso utilizan cifrado asimétrico?
(b) ¿Cuál es el cometido de las autoridades de certificación en la infraestructura PKI?

Cuestión 7.- Las tecnologías DIFFSERV e INTERSERV, tienen un mismo objetivo común. Coméntelo brevemente e indique y las diferencias entre ambas. (0.5 puntos)

Cuestión 8.- Referente al Jitter: (1 punto)

- (a) ¿En qué consiste?
(b) Indique los principales motivos por los que aparece el Jitter.
(c) Proponga y defina alguna forma de medirlo.

Cuestión 9.- Indique las métricas QoS que más afectan a:

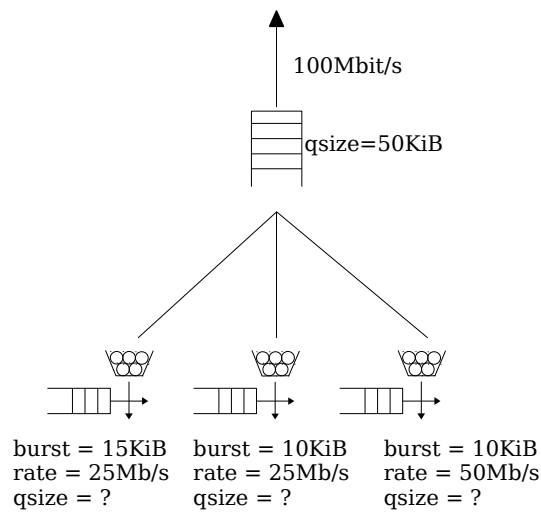
(0.5 puntos)

- (a) Aplicaciones VoIP: _____
- (b) Vídeo bajo demanda: _____

Cuestión 10.- Un router está sirviendo 4 clases de servicios, el router está clasificando usando una política WFQ con quantum: 1, 2, 3 y 4. El enlace de salida tiene una caudal de 30Mbit/s. (1 punto)

- (a) ¿Cual es el caudal mínimo garantizado para cada clase de servicio?
- (b) Calcule el retraso máximo si el tamaño máximo de la cola para cada clase es de 75KiB.

Cuestión 11.- Dado el esquema de cubetas de la figura responda las cuestiones. (1 punto)



- (a) ¿Cual es el caudal mínimo garantizado para cada cubeta?
- (b) Calcule el tamaño de las colas para que el retraso máximo sea 15ms.



Grado en Ingeniería Informática - Tecnologías de la Información
Tecnologías Avanzadas de la Información
Primera convocatoria - Enero de 2017

Apellidos, Nombre: _____



Cuestión 1.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo. Indique en que consiste cada uno de los siguientes ataques y clasifíquelo utilizando la clasificación propuesta en la asignatura. (2 puntos)

- | | |
|--|-------------------------|
| (a) DNS Spoofing | (b) Secuestro de sesión |
| (c) DDOS (Distributed Deny of Service) | (d) Exploit |

Cuestión 2.- Indique las ventajas y los inconvenientes de utilizar un Proxy frente a un Firewall de filtrado de paquetes en el ámbito de la seguridad informática. (0.5 puntos)

Cuestión 3.- Describa brevemente las diferencias entre un Proxy HTTP directo y un Proxy HTTP inverso. (0.5 puntos)

Cuestión 4.- Referente a las infraestructuras de clave pública (PKI) estudiadas en la asignatura, conteste a las siguientes cuestiones: (1.5 puntos)

- (a) ¿Cual es el cometido de las autoridades de certificación en una infraestructura PKI?
- (b) ¿Cual es la diferencia entre una clave pública y un certificado digital?
- (c) ¿Qué es un certificado digital? Indique algunos de sus usos.

Cuestión 5.- A lo largo de la asignatura se ha mostrado el uso de funciones HASH para diferentes propósitos. Responda razonadamente las siguientes cuestiones: (1.5 puntos)

- (a) Indique la diferencia existente entre cifrar un mensaje y aplicar una función HASH al mismo.
- (b) Qué aporta el uso de funciones HASH de contraseñas en los procesos de autenticación de los servicios de red.
- (c) Indique para qué se utilizan las funciones HASH en el proceso de firma electrónica y verificación de la firma electrónica. Utilice un ejemplo para mostrar el proceso de firma electrónica.

Cuestión 6.- Referente al Jitter: (1 punto)

- (a) ¿En qué consiste?
- (b) Indique los principales motivos por los que aparece el Jitter.
- (c) Proponga y defina alguna forma de medirlo.

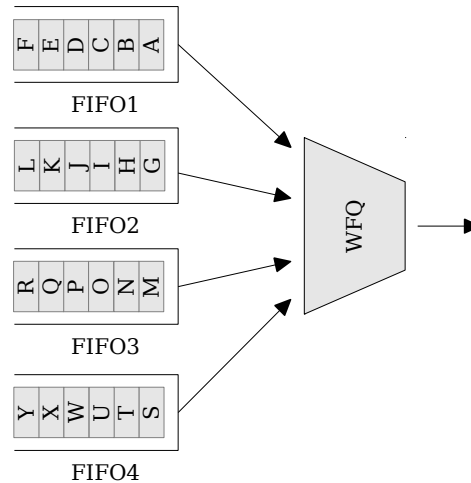
Cuestión 7.- Para cada tipo de aplicación indique cual es la métrica, de las estudiadas en la asignatura, que más afecta a la calidad de dicho servicio, **justificando la respuesta:** (1 punto)

- (a) VOIP
- (b) Vídeo bajo demanda
- (c) IPTV
- (d) Aplicaciones interactivas

Cuestión 8.- En el ámbito de QoS tratado en la asignatura, el uso de un buffer mejora la calidad de servicio de los siguientes tipos de aplicaciones sobre IP: (0.5 puntos)

- Aplicaciones dedicadas a VOIP.
- Aplicaciones de vídeo bajo demanda.
- Juegos interactivos.
- Servidores de contenidos Web.

Cuestión 9.- En el esquema de la figura se ha establecido una política basada en el algoritmo WFQ. (1.5 puntos)



- (a)** Indique el orden en el que salen los paquetes, comenzando por la FIFO1 y con quantums: $q_1=5$, $q_2=3$ y $q_3=2$.
- (b)** Usando los quantum anteriores y con un enlace de salida es de 100Mbit/s, indique el caudal garantizado en cada una de las colas. Use las unidades correctas (Kbit/s, Mbit/s, etc.)
- (c)** Proponga una estructura basada en cubetas con los mismos caudales garantizados. ¿En que mejoran las cubetas al algoritmo WFQ?.



Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Enero de 2017

Apellidos, Nombre: _____



Cuestión 1.- A lo largo del curso en la asignatura se han tratado los siguientes términos en el ámbito de la seguridad informática. Se han agrupado en 6 grupos, describa brevemente cada uno de ellos y la relación existente en cada grupo. (3 puntos)

- | | |
|---|---|
| (a) Proxy - Firewall de filtrado de paquetes | (b) Cifrado simétrico - Cifrado asimétrico |
| (c) Vulnerabilidad - Exploit | (d) VPN - Túnel de red |
| (e) IPSec - SSL/TLS | (f) Botnet - DDOS - DOS |

Cuestión 2.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo como sigue: (1 punto)

- (a)** Ataques a la confidencialidad.
- (b)** Ataques a la autenticidad.
- (c)** Ataques a la disponibilidad.
- (d)** Ataques a la integridad.

Describa brevemente cada uno de ellos y ponga un ejemplo de este tipo de ataques.

Cuestión 3.- La ingeniería social es el origen de la mayoría de los ataques informáticos. Describa brevemente en que consiste e indique cual es la única contramedida efectiva. (0.5 puntos)

Cuestión 4.- A lo largo de la asignatura se ha mostrado el uso de funciones HASH para diferentes propósitos. Responda razonadamente las siguientes cuestiones: (1.5 puntos)

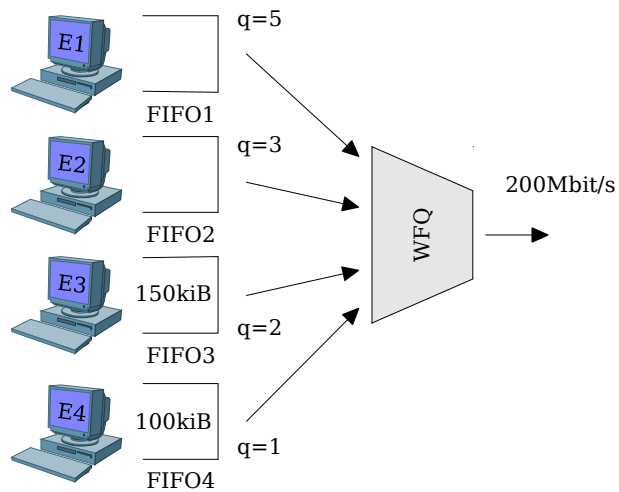
- (a)** Indique la diferencia existente entre cifrar un mensaje y aplicar una función HASH al mismo.
- (b)** Qué aporta el uso de funciones HASH de contraseñas en los procesos de autenticación de los servicios de red.
- (c)** Indique para qué se utilizan las funciones HASH en el proceso de firma electrónica y verificación de la firma electrónica. Utilice un ejemplo para mostrar el proceso de firma electrónica.

Cuestión 5.- Defina los siguientes conceptos: Jitter, capacidad de ruta y capacidad de transporte. (1 punto)

Cuestión 6.- Indique, razonadamente, cuáles de las métricas QoS estudiadas afectan fuertemente a los siguientes servicios/aplicaciones: (1.5 puntos)

- | | |
|--|--|
| (a) Un juego de carreras de coches online | (b) IPTV |
| (c) GMail | (d) Video llamadas con WhatsApp |
| (e) Youtube | (f) Un juego de cartas online |

Cuestión 7.- Dada la configuración mostrada en la figura responda las cuestiones planteadas. (1.5 puntos)



- (a) Indique el caudal garantizado para cada una de los equipos. Use las unidades correctas (Kbit/s, Mbit/s, etc.)
- (b) Calcule el tiempo máximo de espera de los paquetes en la cola 3 y 4.
- (c) Calcule el tamaño máximo de las colas 1 y 2 para que el tiempo de espera de los paquetes no supere 5ms. Expresé el resultado en la unidades: MiB, KiB, etc.



Grado en Ingeniería Informática - Tecnologías de la Información

Tecnologías Avanzadas de la Información - Enero de 2018

Apellidos, Nombre: _____



Cuestión 1.- Según la clasificación de los ataques informáticos propuesto en la signatura, para cada ejemplo indique en que categoría se puede considerar: (1.5 puntos)

- (a) Un secuestro de sesión en un navegador Web se considera un ataque: _____
- (b) Realizar IP spoofing en una red local se considera un ataque: _____
- (c) El RamsomWare se considera un ataque: _____
- (d) Saturar una red local con paquetes UDP se considera un ataque: _____
- (e) Enviar peticiones masivas HTTP desde una botnet contra un servidor WEB se considera un ataque: _____
- (f) Usar un exploit contra un navegador Web vulnerable se considera un ataque: _____

Cuestión 2.- Referente a los ataques informáticos: (1.5 puntos)

- (a) Indique en que consiste el Spoofing.
- (b) Describa cada uno de estos ataques: IP Spoofing, DNS spoofing, Web Spoofing, ARP Spoofing.
- (c) Indique cuales de los ataques del apartado (b) sólo se pueden realizar en una red local.

Cuestión 3.- En las prácticas de laboratorio se ha creado una red de 3 equipos, uno de ellos con un firewall, indique a que tipo de configuración de las estudiadas corresponde: (0.5 puntos)

- Dual-Homed gateway.
- Screened host.
- DMZ Screened Subnet.

Cuestión 4.- En los routers actuales existe una opción de configuración llamada DMZ que hace referencia a *DeMilitarized Zone*. Comente brevemente en que consiste y cual es el efecto cuando se activa. (0.5 puntos)

Cuestión 5.- En el ámbito de la seguridad informática las funciones HASH se utilizan: (1 punto)

- En los procesos de autenticación con contraseña.
- Para cifrar datos en una comunicación de red.
- En el proceso de firma electrónica.
- En los certificados digitales usados con el protocolo SSL.

Cuestión 6.- Referente a los PKIs, una vez generada una clave pública y una privada ¿En qué consiste el proceso de generar un Certificado Digital por parte de una Autoridad de Certificación? (0.5 puntos)

Cuestión 7.- Respecto al cifrado asimétrico, certificados digitales y PKIs, indique las afirmaciones que son correctas: (1 punto)

- Para verificar una firma electrónica es necesaria la clave privada del firmante.
- Los datos cifrados con la clave privada sólo se pueden descifrar con la clave pública.
- Los datos cifrados con la clave pública sólo se pueden descifrar con la clave privada.
- El cifrado simétrico es más lento que el cifrado asimétrico.
- El cifrado simétrico es más seguro que el cifrado asimétrico.
- En multitud de protocolos, como por ejemplo IPSec, el cifrado asimétrico sólo se usa para intercambiar claves simétricas, y después, se cifran los datos sólo con claves simétricas.

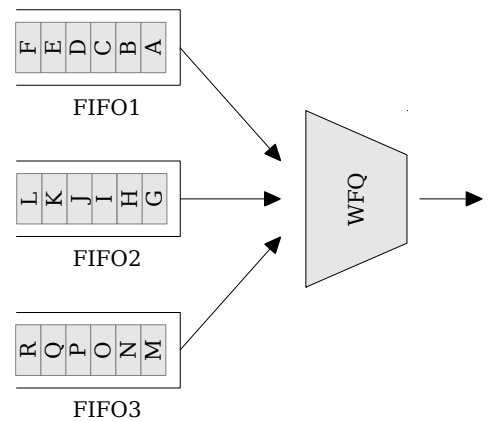
Cuestión 8.- Describa brevemente en que consiste un túnel de red en el ámbito de la asignatura y para que ha sido utilizado. (0.5 puntos)

Cuestión 9.- En el ámbito de QoS tratado en la asignatura: (1 punto)

- (a) Describa brevemente 3 métricas de las estudiadas en la asignatura.
- (b) Para cada métrica del apartado (b) indique 2 aplicaciones cuya calidad de servicio se ve afectada fuertemente por dicha métrica.

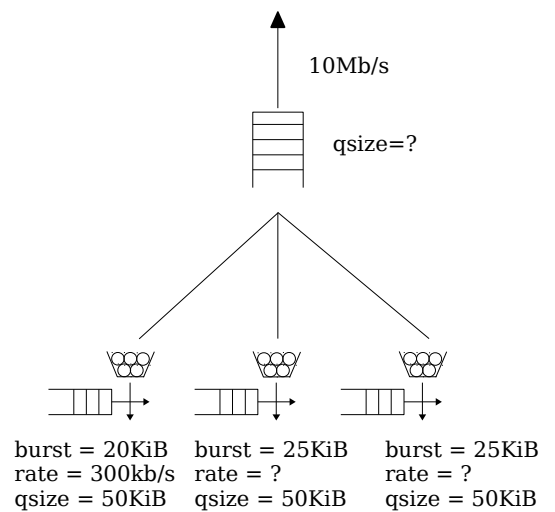
Cuestión 10.- En el esquema de la figura se ha establecido una política basada en el algoritmo WFQ. (1 punto)

- (a) Indique el orden en el que salen los paquetes, comenzando por la FIFO1 y con quantums: $q_1=4$, $q_2=3$ y $q_3=1$.
- (b) Si el enlace de salida es de 300Mbit/s calcule el tamaño de cada cola para que el tiempo de espera máximo sea inferior a 5ms usando los quantums anteriores. Indique el resultado en las unidades KiBytes / MiBytes.



Cuestión 11.- Dada la configuración de cubetas mostrada en la figura responda las siguientes cuestiones. (1 punto)

- (a) ¿Cuál es el mínimo tamaño de la cola de salida ($qsize$) para que la configuración de la figura opere correctamente? Justifique la respuesta.
- (b) ¿Cuál es la restricción existente para configurar la velocidad de las cubetas (parámetro $rate$)? Justifique la respuesta y proponga una solución.





Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Febrero de 2018

Apellidos, Nombre: _____



Cuestión 1.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo, indique cuál es la clasificación propuesta y ponga un ejemplo de cada tipo de ataque. *(1 punto)*

Cuestión 2.- La ingeniería social es el origen de la mayoría de los ataques informáticos. Describa brevemente en que consiste e indique cual es la única contramedida efectiva. *(0.5 puntos)*

Cuestión 3.- Señale las afirmaciones correctas: *(1 punto)*

- Un firewall de filtrado de paquetes protege de los ataques provenientes de la red interna.
- Un proxy protege de ataques de ingeniería social.
- Un firewall de filtrado de paquetes opera con menos recursos que un proxy.
- Un proxy se puede utilizar para realizar operaciones de filtrado en el nivel de aplicación.
- Un firewall de filtrado de paquetes trabaja a nivel de aplicación.
- Un firewall de filtrado de paquetes trabaja a nivel de red.

Cuestión 4.- En el ámbito de la seguridad informática las funciones HASH se utilizan: *(0.5 puntos)*

- En los procesos de autenticación con contraseña.
- Para cifrar datos en una comunicación de red.
- En el proceso de firma electrónica.
- En los certificados digitales usados con el protocolo SSL.

Cuestión 5.- En la asignatura se ha dedicado un tema al estudio de las VPNs. En él que se mostraban diferentes tecnologías usadas. Describa brevemente en que consiste cada una de las siguientes e indique que relación tiene con una VPN: *(1 punto)*

- (a) Túnel de red. (b) Cifrado simétrico. (c) Cifrado asimétrico. (d) IPSec.

Cuestión 6.- Referente a los PKIs, una vez generada una clave pública y una privada ¿En qué consiste el proceso de generar un Certificado Digital por parte de una Autoridad de Certificación? *(0.5 puntos)*

Cuestión 7.- Comente brevemente que aporta el uso de una VPN frente al uso de una simple comunicación cifrada como podría ser SSH, SSL, FTPS, etc. *(1 punto)*

Cuestión 8.- La tecnología DIFFSERV tiene como objetivo dotar a Internet de QoS mediante el marcado de paquetes, responda brevemente: *(1 punto)*

- (a) ¿En que consiste el marcado de paquetes?
- (b) ¿Qué tecnología diferente al marcado de paquetes usa INTERSERV y por qué fracaso?

Cuestión 9.- Referente al Jitter: *(1 punto)*

- (a) ¿En qué consiste?
- (b) Indique los principales motivos por los que aparece el Jitter.
- (c) Proponga y defina alguna forma de medirlo.

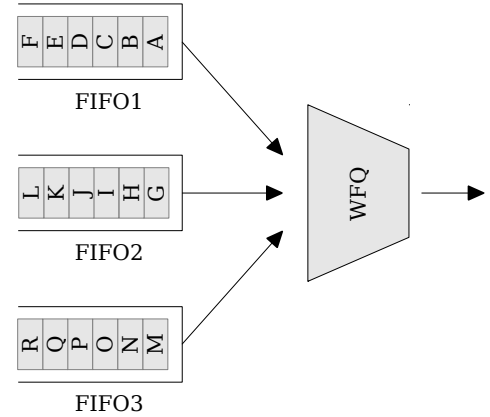
Cuestión 10.- Indique las métricas QoS estudiadas que más afectan a las siguientes aplicaciones concretas: (1 punto)

- | | | | |
|--------------|-------------|-------------|-----------------------------|
| (a) Skype | (b) Youtube | (c) Netflix | (d) Mensajería con WhatsApp |
| (e) FaceBook | (f) Gmail | (g) FTP | (h) SSH |

Cuestión 11.- En el esquema de la figura se ha establecido una política basada en el algoritmo WFQ.

(1.5 puntos)

- (a) Indique el orden en el que salen los paquetes, comenzando por la FIFO1 y con quantums: $q_1=5$, $q_2=3$ y $q_3=1$.
- (b) Si el enlace de salida es de 50Mbit/s indique para cada cola cual es caudal máximo garantizado y la tasa pico.
- (c) Calcule el tamaño de cada cola para que el tiempo de espera máximo sea inferior a 10ms usando los quantums anteriores. Indique el resultado en las unidades KiBytes / MiBytes.





Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Evaluación continua 2019

Apellidos, Nombre: _____



Cuestión 1.- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo, indique cuál es la clasificación propuesta y ponga un ejemplo de cada tipo de ataque. *(1 punto)*

Cuestión 2.- Indique las diferencias entre los ataques informáticos estructurados y los no estructurados. *(0.25 puntos)*

Cuestión 3.- Indique que tipo de ataque informático es un escaneo de puertos. *(0.25 puntos)*

Cuestión 4.- Los ataques DoS principalmente son de 2 tipos. Describa brevemente en que consisten ambos tipos. *(1 punto)*

Cuestión 5.- Un ataque típico en una red local es la inundación con paquetes UDP. En las redes IP los protocolos no tienen prioridad, entonces ¿por qué el efecto de la inundación UDP es la anulación del protocolo TCP? *(0.5 puntos)*

Cuestión 6.- OpenVPN utiliza las tecnologías indicadas. Describa brevemente cada una de ellas e indique para qué se utiliza en las VPNs *(1.5 puntos)*

- (a) Claves públicas y privadas RSA.
- (b) PKI: Certificados digitales, autoridades de certificación y firma electrónica.
- (c) Cifrado asimétrico.
- (d) Cifrado simétrico.
- (e) Túnel de red.
- (f) Protocolo TLS/SSL.

Cuestión 7.- En el ámbito de la seguridad informática las funciones HASH se utilizan: *(1 punto)*

- En los procesos de autenticación con contraseña.
- Para cifrar contraseñas.
- Para cifrar datos en una comunicación de red.
- En el proceso de firma electrónica.
- En la tecnología blockchain.
- En los certificados digitales usados en el protocolo SSL/TLS.

Cuestión 8.- Describa brevemente que es el Jitter e indique los principales motivos por los que aparece. *(0.5 puntos)*

Cuestión 9.- La tecnología DIFFSERV tiene como objetivo dotar a Internet de QoS mediante el marcado de paquetes, responda brevemente: *(1 punto)*

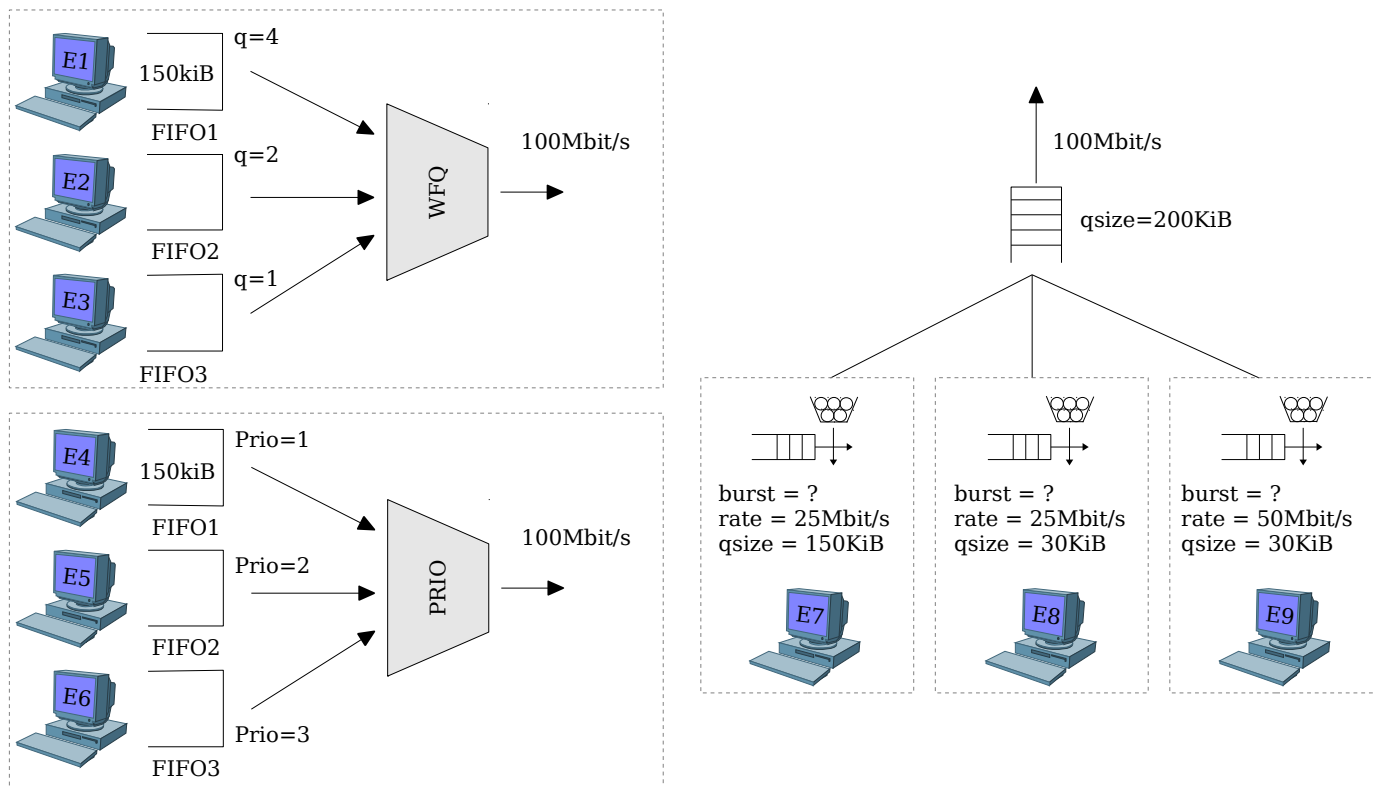
- (a) ¿En que consiste el marcado de paquetes?
- (b) ¿Qué tecnología diferente al marcado de paquetes usa INTERSERV y por qué fracaso?

Cuestión 10.- Indique las métricas QoS estudiadas que más afectan a las siguientes aplicaciones: *(1 punto)*

- (a) Skype
- (b) Youtube
- (c) Netflix
- (d) Minecraft
- (e) FaceBook
- (f) Gmail
- (g) SFTP
- (h) Canal de deportes IPTV

Cuestión 11.- En la figura se muestran tres configuraciones:

(2 puntos)



(a) Rellene la tabla indicando el mínimo caudal garantizado y la tasa pico usando las unidades correctas (G,M,K, etc.)

Equipo	E1	E2	E3	E4	E5	E6	E7	E8	E9
Caudal mínimo garantizado									
Caudal máximo (tasa pico)									

- (b) Calcule el retraso máximo en los equipos E1 y E4.
- (c) Calcule el tamaño de la cola del equipo E3 para que tenga un retraso máximo de 25ms.
- (d) Para la configuración con cubetas proponga una configuración para las ráfagas de cada equipo (parámetros burst) que no genere problemas de funcionamiento. ¿cual es la restricción existente cuando se configura el parámetro *burst*?



Grado en Ingeniería Informática - Tecnologías de la Información Tecnologías Avanzadas de la Información - Enero 2019

Apellidos, Nombre: _____



Cuestión 1.- Usando la clasificación de los ataques informáticos propuesto en la asignatura, para cada ejemplo indique en que categoría se puede incluir: *(1.25 puntos)*

- (a) Un secuestro de sesión en un navegador Web: _____
- (b) Saturar una red local con paquetes UDP: _____
- (c) Usar un exploit contra un navegador Web vulnerable: _____
- (d) Un ataque con Ransomware: _____
- (e) Suplantar una Web mediante WebSpoofing: _____

Cuestión 2.- La ingeniería social es el origen de la mayoría de los ataques informáticos. Describa brevemente en que consiste e indique cual es la única contramedida efectiva. *(0.25 puntos)*

Cuestión 3.- Referente a los ataques informáticos comente brevemente en que consiste cada uno de los siguientes: *(1 punto)*

- (a) Malware
- (b) Ransomware
- (c) Keylogger
- (d) Escaneo de puertos con NMAP

Cuestión 4.- OpenVPN utiliza las tecnologías indicadas. Describa brevemente cada una de ellas e indique para qué se utiliza en las VPNs *(1.5 puntos)*

- (a) PKI: Certificados digitales, autoridades de certificación y firma electrónica.
- (b) CRL: Certificate Revocation List (lista de revocación de certificados).
- (c) Cifrado asimétrico.
- (d) Cifrado simétrico.
- (e) Túnel de red.
- (f) Protocolo TLS/SSL.

Cuestión 5.- Marque las afirmaciones correctas *(0.5 puntos)*

- Uno de los usos de las funciones HASH es el cifrado de contraseñas.
- En las infraestructuras PKI, los certificados están firmados con la clave pública de una Autoridad de certificación.
- El protocolo SSL/TLS hace uso de un PKI con certificados digitales.
- Para verificar una firma electrónica es necesaria la clave pública del firmante.

Cuestión 6.- Los ataques DoS principalmente son de 2 tipos. Indique cuales son y coméntelos brevemente. *(1 punto)*

Cuestión 7.- En el proceso de firma electrónica se utilizan las siguientes tecnologías: cifrado asimétrico y funciones HASH. Explique en que consiste el proceso de firma y para que se usa cada una de las tecnologías indicadas. Para mayor claridad, proponga un ejemplo. *(1 punto)*

Cuestión 8.- Defina los siguientes conceptos: Jitter, capacidad de ruta y capacidad de transporte. *(0.5 puntos)*

Cuestión 9.- Indique las métricas QoS estudiadas que más afectan a las siguientes aplicaciones concretas: (1 punto)

- | | | | |
|-------------------|-------------|----------|-----------------------------|
| (a) Videollamadas | (b) Youtube | (c) IPTV | (d) Mensajería con WhatsApp |
| (e) FaceBook | (f) Gmail | (g) FTP | (h) SSH |

Cuestión 10.- En el esquema de la figura se ha establecido una política basada en el algoritmo WFQ.

(1.5 puntos)

- (a) Indique el orden en el que salen los paquetes, comenzando por la FIFO1 y con quantums: $q_1=3$, $q_2=2$ y $q_3=2$.
- (b) Si el enlace de salida es de 25Mbit/s indique para cada cola cual es caudal mínimo garantizado y la tasa pico.
- (c) Calcule el tamaño de cada cola para que el tiempo de espera máximo sea inferior a 15ms usando los quantums anteriores. Indique el resultado en las unidades KiBytes / MiBytes.

