Departamento de Ingeniería Telemática y Electrónica

EXAMEN 2º PARCIAL DE ADMINISTRACIÓN DE REDES Y SISTEMAS

1 - JUNIO - 2017

Notas previas:

- **NO** se permite la utilización de ningún tipo de documentación en el examen.
- **DURACIÓN: 45 minutos**
- Publicación de notas: **9-junio-2017**. Revisión **11-junio-2017 12:30h**

--- SOLUCIÓN ---

Cuestión 1: (1,5 puntos). En el contexto del servicio de compartición de disco en red mediante NFS:

a) Indique si este servicio se clasificaría como de tipo NAS o SAN y porqué.
NAS. Servicio de compartición de ficheros, no de bloques.

b) Indique qué demonios mínimos debería tener en ejecución un servidor NFS para que un cliente pueda llegar a leer un fichero alojado en uno de sus recursos exportados.
rpcbind, nfsd, mountd.

c) Un sistema A exporta mediante NFS un directorio "/export" (uid 0, gid 0, máscara "rwxr-xr-x") y un sistema B lo ha montado vía NFS con éxito. Este directorio contiene un fichero normal "f.txt" (uid 1001, gid 200, máscara "rwxr-x---"). Sin alterar los atributos indicados, y teniendo en cuenta solo cuestiones relativas a permisos y el funcionamiento y configuración de NFS, ¿podría afirmar con certeza que el usuario "root" (uid 0, gid 0) de B no tiene permisos para leer ese fichero? Tanto si afirma que root no podría leerlo, como si no (sí podría leerlo) es imprescindible que indique el motivo que lo podría estar impidiendo o permitiendo, respectivamente.
No. Depende de parámetro de exportación maproot

Cuestión 2: (4 puntos) En el contexto del correo electrónico:

a) ¿Para qué sirve una estafeta secundaria? ¿Cómo se puede saber que es secundaria y no primaria o de otro tipo?
Recibir correo-e dirigido al dominio, como respaldo de la primaria. El registro MX de la primaria es el menor valor de los existentes.

b) ¿Qué estafetas existentes un dominio dado –primaria, secundaria, *smarthost*, satélite--, requieren acceso a los buzones de los usuarios?
Primaria.

c) Una estafeta de entrada es primaria para el dominio @upm.es. Si recibe mediante SMTP un mensaje dirigido a x@google.es, indique por qué, en general, no debería tramitarlo e indique y explique **tres** casos (o configuraciones de la estafeta) en los que, por el contrario, sí debería aceptarlo y tramitarlo. Y si la estafeta de entrada fuera secundaria para el dominio @upm.es, ¿debería aceptarlo y tramitarlo?
En general no debería tramitarlo porque podrían estar usándola para enviar spam dirigido a @google.es. Algunos casos en que sí debería tramitarlo pueden ser: 1) El correo se recibe desde un sistema de confianza (p.e., porque su IP aparece en el my_networks de Postfix o similar). 2) El correo es entregado por un usuario autenticado de @upm.es 3) La estafeta es secundaria del dominio @google.es.

d) Explique cuando se usa una estafeta postfix y el software amavis:
   a. ¿Para qué sirve la etiqueta *content-filter* asociada a un proceso smtpd?.
   Para que dicho añada la etiqueta a los mensajes de correo entrantes, el servicio a través del filtro que especifica la etiqueta, como por ejemplo un antispam o antivirus.

b. Para qué sirven las colas *incoming*, *active*, *deferred*. Si un usuario local de la estafeta envía un correo-e a pepe@noexiste.es y este dominio @noexiste.es no existe en el DNS, indique por cuáles de estas colas pasaría ese mensaje.
Incoming: se depositan nuevos mensajes; *active*: mensajes que se están intentando enviar, *deferred:* mensajes que tras algún intento de envío, no han podido ser enviados y están esperando el momento de su reintento. Incoming->active.

Cuestión 3: **(4,5 puntos)** En el contexto del servicio web ofrecido mediante software apache:

a) Ante una petición HTTP detalle el mecanismo que permite a un servidor web ofrecer sitios virtuales. ¿Por qué, por defecto, no es aplicable a HTTPS?

Las peticiones HTTP tienen una cabecera llamada "Host" en la que el cliente indica a qué sitio corresponde la petición. El servidor web usa esa cabecera para seleccionar la configuración correspondiente al sitio web en cuestión (identificado por el parámetro "ServerName") y así puede albergar múltiples sitios virtuales independientes.
En el HTTPS original, primero se realiza la fase de negociación del protocolo SSL, en la cual el servidor presenta un certificado X.509, y después se realizar la fase de protocolo HTTP. Por tanto, en la fase de SSL no se sabe todavía para qué sitio web será la petición (pues eso se sabrá al llegar a la fase de HTTP) y no se puede presentar el certificado correspondiente, si es que hay varios. Para solventar la dificultad anterior, se añadió al protocolo SSL una opción llamada SNI ("Server Name Indication") con la que el cliente SSL puede decirle al servidor SSL el nombre de sitio que usará en la fase de HTTP.

b) Explique la diferencia de funcionamiento, cuando se accede a http://www.ejemplo.es/videos, si el servidor configura 1) un "Redirect /videos http://www.multimedia.es/videos" o 2) un proxy inverso de /videos a http://www.multimedia.es/videos"

Redirect devuelve al cliente una respuesta HTTP en la que le indica que haga una nueva petición al URL /videos /multimedia/videos. Alias hace que el servidor internamente resuelva la solicitud desde /videos a http://www.multimedia.es/videos sin que el cliente sea consciente de dicho cambio.

c) Si el administrador del sitio web www.ejemplo.es quiere habilitar el acceso cifrado mediante HTTPS y que funcione sin avisos para un usuario que navega con cliente Firefox, ¿qué dos características fundamentales debe tener el correspondiente certificado X.509?

El certificado debe corresponder al commonName www.ejemplo.es. Para el caso concreto de Firefox, que el certificado se encuentre firmado por una CA cuya clave pública esté incluida en la lista de CA que se distribuye con Firefox (o firmado por una CA subordinada de alguna otra que cumpla esta condición).

d) Un usuario A escribe en su navegador web el URL ***http****://www.upm.es/blog/index.php* y otro usuario B escribe ***https****://www.upm.es/blog/index.php*. Si ambos usuarios realizan su petición, y www.upm.es se resuelve siempre como IP 3.3.3.5, explique motivadamente si se podría o no afirmar (para rebatirlo puede describir algún ejemplo de arquitectura/configuración en la que no sucede lo que se afirma):

i. Que la respuesta HTTP que recibe cada usuario siempre es generada por un mismo servidor web.
No, p.e. podrían existir mecanismos a nivel de transporte (como NAT,…) que impliquen que atiende cada vez un servidor web distinto.

ii. Que el contenido HTML (respuestas HTTP con estado 200 -éxito-) siempre es generado por el mismo servidor web.
No, p.e. podrían existir un proxy web inverso repartiendo peticiones a diferentes servidores web para generar el contenido.

iii. Que el contenido HTML (respuestas HTTP con estado 200 –éxito-) que reciben ambos usuarios siempre es idéntico.

No, p.ej, los servidores de la respuesta ii podrían estar desincronizados, o el contenido HTML contener referencias locales como https en un caso y http en el otro.

iv. Que el contenido HTML (en respuestas HTTP con código 200 éxito)-que reciben ambos usuarios, si el administrador de UPM siempre configurar servidores web virtuales distintos para atender por separado las peticiones dirigidas a los puertos 443/tcp (https) y 80/tcp (http), nunca podría ser generado por un mismo servidor virtual.
No, p.ej, el servidor web que atiende 443/tcp (https) podría ser un proxy web que termine el cifrado mediante SSL, e internamente redirija la petición vía http al servidor virtual en 80/tcp para generar el contenido.

e) Indique los tres errores que presenta la siguiente configuración mínima de un sitio virtual para http://www.etsist.upm.es

```
<VirtualHost *:80>
        ServerName www.etsist.upm.es
        DocumentRoot /usr/local/www/data/www.etsist.upm.es
        <Directory /usr/local/www/data/www.etsist.upm.es>
                Allow from all
                Require all granted
        </Directory>
</VirtualHost>
```