1) ¿Qué comando usuarias para lanzar manualmente el aprendizaje de Spamassessin sobre los mensajes de "Junk" y "no-Junk"? (2 puntos)

- zmupdatespam
- zmtrainsa
- zmantispamctl
- zmprov renew spam

Respuesta:
http://wiki.zimbra.com/index.php?title=CLI_zmtrainsa#5.0.2
El script zmtrainsa se lanza cada dia por la noche desde un cron para leer las cuentas de ham y spam.

2) ¿Qué es un registro de DNS de tipo SPF? (2 puntos)

- Es un nuevo tipo de registro en el DNS que especifica cuales son las direcciones desde donde se puede enviar correo de un dominio concreto.
- Es un registro del DNS que contiene la lista de MTAs que aceptan correo de un dominio.
- Es un registro del DNS que contiene la información sobre una zona.
- Es un registro del DNS llamado Service Policy False que indica cuando un dominio es falso.

Respuesta:
http://es.wikipedia.org/wiki/SPF
Se trata de un nuevo registro que surgió como propuesta para combatir el spam y el phishing.
Ver el RFC4408 del abril 2006.

3) Estamos debugeando un servidor con un Telnet al 25. ¿Cómo empieza y acaba el cuerpo del mensaje? (2 puntos)

- Empieza por el comando DATA y finaliza con un punto.
- Empieza con el comando SEND y finaliza con un punto
- Empieza con el comando DATA y finaliza con un punto y coma
- Empieza con un DATA y finaliza con la ultima linea del mensaje.

Respuesta:
http://es.wikipedia.org/wiki/SMTP
Ver el RFC0821 de agosto de 1982.

4) A la vista de la siguiente imagen. Suponiendo que quiero enviar un correo a @sun.com y que todos sus MTA están online, ¿por donde se enviará el correo? (3 puntos)

- Por btmx4.sun.com o por btmx6.sun.com
- Por bt4mx.sun.com
- Por 192.18.98.36 o 192.118.98.34
- Ninguna de las anteriores respuestas es correcta.

Respuesta:
http://es.wikipedia.org/wiki/MX_(registro)
Como todos los MTAs están online, el correo se enviará por el de menor peso (5). Dado que hay dos MTAs con peso 5, el correo se enviará por uno u otro. No es posible determinar a priori por cual se envía.

5) Según este Log (ver zimbra.log.zip), porqué Cruz García de IBM no recibió su ultimo correo. (5 puntos)

- El MTA del remitente no pudo contactar con el servidor de IBM.
- Lo rechazó el servidor porque el usuario tenía el buzón lleno.
- Lo rechazó el servidor porque el remitente se equivocó al escribir la dirección de correo de Cruz.
- Lo rechazó el servidor porque el mensaje contenía un virus.
- Ninguna de las anteriores.

Respuesta:
Ve la línea 19.687. Se rechazó el correo por tener un adjunto peligroso. Notar que la primera respuesta es totalmente absurda. Si no se puede contactar con el servidor de IBM este no puede anotarlo en su log.

6) ¿Cual de los siguientes métodos es el recomendado por Zimbra para migrar el buzón de un servidor Zimbra Open a otro Zimbra Open? (2 puntos).

- imapsync y abriendo el puerto 110 en el destino.
- imapsync y abriendo el puerto 143 en el destino
- pop2imap y abriendo el 143 en el destino
- Copiando directamente las carpetas y archivos de los mailboxes de un servidor al otro.

Respuesta
http://wiki.zimbra.com/index.php?title=User_Migration#Migrating_from_an_existing_IMAP_server_.28Recommended_Method.29
La Wiki oficial de Zimbra recomienda utilizar un método basado en IMAP.

7) Estamos debugeando un servidor con un Telnet al 110.

```
+OK zimbra.ibm.com Zimbra POP3 server ready
user amperis
+OK hello amperis, please enter your password
pass perro45%
+OK server ready
stat
+OK 3 110670
list
+OK 3 messages
1 9461
2 93871
3 7338
.
```

¿Qué comando utilizamos para eliminar el correo más grande? (2 puntos)

- DELETE 3
- DELE 2
- DELE 2 y luego un QUIT
- DELE 2 y luego un RSET

Respuesta:
http://pages.prodigy.net/michael_santovec/pop3telnet.htm
Para eliminar un correo es necesario hacer un DELE y al finalizar un QUIT. Sólo con el QUIT se confirma la eliminación del mensaje. Si hacemos un DELE y se pierde la conexión no se eliminará ningún mensaje. Ver también el RFC1939.

8) Los filtros bayesianos como los de Spamassessin funcionan con la probabilidad de que un suceso futuro está condicionado y puede ser deducible de las apariciones previas de este mismo suceso en el pasado.
¿Cuantos correos detectados como spam y cuantos correos detectados como legítimos necesita Spamassessin para empezar a aplicar lógica bayesiana? (3 puntos)

- 500 spam y 150 legítimos
- No necesita ninguna cantidad especifica.
- 500 spam y 400 legítimos.
- 200 spam y 200 legítimos

Respuesta:
http://wiki.apache.org/spamassassin/BayesInSpamAssassin

9) Si en Zimbra tenemos instalado el módulo de Logger, este cada día mediante un cron enviará un report de los errores generados, el número total de mensajes y también los usuarios que más envian y reciben correo. Por defecto este límite está acotado a los 50 usuarios más activos.
¿Qué comando utilizamos para reducir o aumentar este listado de usuarios más activos? (2 puntos)

- Un zmprov
- Un zmlocalconfig
- Modificado un parámetro dentro del fichero de configuración logger.cf.in
- Modificando un parámetro dentro del fichero de configuración amavisd.conf.in

Respuesta:
http://www.zimbra.com/docs/ne/latest/administration_guide/9_Monitoring.14.1.html
Podemos utilizar "zmlocalconfig -e zimbra_mtareport_max_recipients=<number>" o "zmlocalconfig -e zimbra_mtareport_max_senderss=<number>"

10) Cual es el reverseDNS de la IP 64.233.165.25. (2 puntos)

- jl-in-f25.google.com
- smtp2.google.com
- mx2.google.com
- 25.165.233.64.in-addr.arpa.
- Ninguna de las anteriores

Respuesta:
Utilizar el comando "dig –x 64.233.165.25" o http://remote.12dt.com/lookup.php

11) Supongamos el siguiente cuerpo del mensaje:

```
…
X-Spam-Status: ???, score=8.436 tagged_above=??? required=???
tests=[BAYES_50=0.001, DNS_FROM_RFC_BOGUSMX=1.482,
RCVD_IN_BL_SPAMCOP_NET=1.96, RCVD_IN_PBL=0.905, RCVD_IN_XBL=2.033,
RDNS_NONE=0.1, URIBL_BLACK=1.955]
…
From: "Facebook Update Center" <user@facebook.com>
To: <amperis@ibm.com>
```

Y que nuestro Zimbra está configurado con los siguientes valores:

zimbraSpamKillPercent: 25
zimbraSpamTagPercent: 10

¿El mensaje que se envía desde Facebook será considerado spam? (3 puntos)

- El correo será marcado como spam
- El correo no será marcado como spam
- El correo será eliminado
- 25 y 10 no son valores posibles.

Respuesta:
http://amperis.blogspot.com/2008/04/zimbra-y-spamassession-bajar-los.html

12) A la vista de la siguiente configuración de un router Cisco (ver startup-config.txt.zip).

¿Por qué lo usuarios conectados desde Internet no pueden descargarse su correo en sus Outlooks? Según conversación con uno de estos usuarios dice: "… el correo dice fallo de conexión con el servidor". (3 puntos)

- El siguiente NAT está mal configurado: "ip nat inside source static tcp 10.1.0.3 267 224.57.124.3 25 extendable".
- Porque la lista de acceso 150 no esta bien aplicada a la interfaz ATM.
- Porque la limitación del ancho de banda en la interfaz de ATM no deja descargar el tráfico del correo.
- Ninguna de las anteriores.

Respuesta:
Para descargar el correo faltaría un NAT desde el puerto 110 o 143 al servidor de correo..

13) ¿Cual de las siguientes configuraciones es correcta para un registro SPF para el dominio microsoft.com que indique que su máquinas de correo autorizadas son todas las de sus MX más la maquina 65.55.88.22? (3 puntos)

- microsoft.com. IN TXT "v=spf1 mx ip4:65.55.88.22 ~all"
- microsoft.com. IN TXT "v=spf1 mx=100 ip=65.55.88.22~all"
- microsoft.com. IN SPF "mx ip=65.55.88.22~all"
- microsoft.com. IN SPF "mx and ip=65.55.88.22and ~all"
- microsoft.com. IN SPF "mx and ip=65.55.88.22"
- microsoft.com. IN SPF "v=spf1 mx a:mail.global.frontbridge.com ~all"
- La opción primera y la opción sexta son correctas

Respuesta:
http://old.openspf.org/wizard.html
Para incluir información dentro de SPF (Sender Policy Framework) se utiliza un tipo de registros de información textual llamado TXT. Dentro de el se configura la información de SPF. Ver el RFC 4408. También es posible utilizar "IN SPF" tal como indica el RFC.