Preguntas Examen LDAP, Correo y Web

Pregunta 1

Finalizado

Se puntúa 0.26 sobre 0.35

Los objetos del directorio se organizan en un [árbol jerárquico] .

Cada objeto se identifica por medio de un [distinguished name (DN)] .

El esquema define [clases de objetos] .

El servicio de directorio obliga a que todos los accesos se hagan [autenticados] .

[esquema] [servidor maestro]

[object identifier (OID)] [common name (CN)]

[filtros de búsqueda] [modos de acceso]

[mediante TCP] [cifrados]

Pregunta 2

Finalizado

Se puntúa 0.26 sobre 0.35

Cada clase de objetos define un conjunto de posibles [atributos] .

Los atributos pueden ser [multivaluados] .

Los OID (object identifiers) identifican a [clases de objetos y atributos] .

Las unidades organizativas (OU) son [nodos base del árbol de directorio]

[esquemas] [filtros de acceso]

[distribuidos] [replicados]

[tipos de esquemas] [objetos individuales del directorio]

[contenedores de objetos]

[puntos para enganchar ramas distribuidas del directorio]

Pregunta **3**

Sin contestar

Puntúa como 0.20

En el directorio LDAP, ¿qué se entiende por "distribución" y qué se entiende por "replicación"?

Distribución:

En el contexto de un directorio LDAP, la "distribución" se refiere a cómo se estructuran y se organizan los datos dentro del directorio. Esto incluye la forma en que se definen las unidades organizativas (OUs), los grupos y los objetos individuales (como usuarios, equipos, etc.).

Replicación:

La "replicación" en un entorno LDAP es el proceso mediante el cual se copian y se sincronizan los datos entre múltiples servidores LDAP. Esto se hace para mejorar la disponibilidad, la escalabilidad y la redundancia de los datos en un entorno distribuido. La replicación garantiza que los datos estén disponibles en varios servidores, lo que permite un acceso rápido y confiable, así como una tolerancia a fallos. Los cambios realizados en un servidor se propagan a otros servidores mediante el proceso de replicación, asegurando que todos los servidores tengan una copia actualizada de los datos.

En resumen, la distribución se refiere a la organización de los datos dentro del directorio LDAP, mientras que la replicación se refiere a la copia y sincronización de esos datos entre múltiples servidores LDAP para mejorar la disponibilidad y la redundancia.

Pregunta **4**

Finalizado

Puntúa como 0.40

Sea un mensaje de correo electrónico que se está intercambiando entre dos estafetas.

a) Ponga un ejemplo en el que el sobre contenga una dirección que no aparece en la cabecera To:. Si eso es imposible, explique por qué.

b) Ponga un ejemplo en el que la cabecera To: contenga una dirección que no aparece en el sobre. Si eso es imposible, explique por qué.

a) Ejemplo en el que el sobre contiene una dirección que no aparece en la cabecera To:

Por ejemplo si Bob quiere enviar un mensaje a Pepe y Alice, pero no quiere que Alice sepa o vea que el mensaje ha sido enviado también a Pepe, Bob pondrá en el campo to: la dirección de Alice y en el campo bcc : Pepe. De esta forma el mensaje se enviará a las 2 direcciones pero Alice solo verá a el como único destinatario.

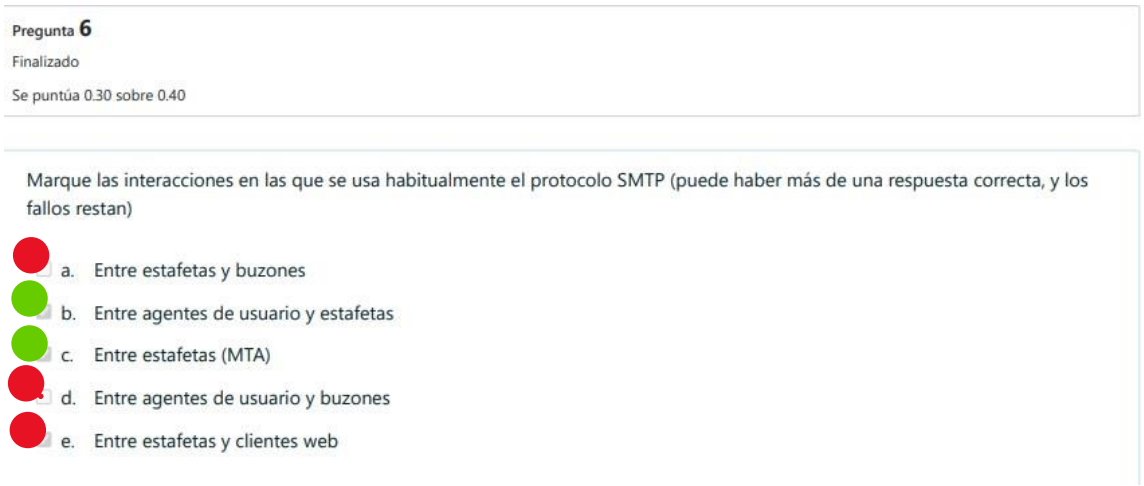
b) Ponga un ejemplo en el que la cabecera To: contenga una dirección que no aparece en el sobre. Si eso es imposible, explique por qué.

Es imposible ya que el sobre debe contener todas las direcciones que hay en los campos

To, cc y bcc.

Nslookup -type=MX ucm.es

1. **Conexión inicial:** La estafeta intentará conectarse a la máquina **aspmx.l.google.com**, que es el servidor de correo especificado en los registros MX (Mail Exchange) del dominio **ucm.es**. Google utiliza servidores MX con ese nombre para gestionar el correo electrónico entrante para algunos dominios, incluidos aquellos que utilizan Google Workspace (anteriormente conocido como G Suite). Entonces, esa sería la primera máquina a la que intentaría conectarse la estafeta.
2. **Si la máquina no responde:** Si **aspmx.l.google.com** no responde (por ejemplo, debido a problemas de red o a la no disponibilidad del servidor en ese momento), la estafeta intentará conectarse a otra máquina de correo que pueda estar especificada en los registros MX del dominio **ucm.es**. Los registros MX generalmente tienen varias entradas, que se priorizan para la entrega del correo. La estafeta intentará conectarse a la siguiente máquina según la prioridad establecida en los registros MX.
3. **Si la máquina de destino devuelve un código 4xx:** Un código de estado de la forma 4xx indica un error del lado del cliente, lo que podría significar que la dirección de correo electrónico no existe en el servidor destino, o podría haber algún otro problema de configuración. En este caso, la estafeta debe enviar un informe de notificación de entrega (DSN) al remitente, informándole del error de entrega. Luego, descartará el mensaje ya que no pudo ser entregado con éxito.



1. **La IP del PC infectado aparece en una lista del tipo DNSBL**: Esta medida sería bastante eficaz. Las listas DNSBL (Listas Negras de Servidores de Correo) se utilizan comúnmente para identificar y bloquear servidores conocidos por enviar spam. Si la IP del PC infectado está en una lista DNSBL, es probable que los servidores de destino lo detecten y marquen los mensajes como spam o los descarten directamente.
2. **El dominio de origen tiene un registro SPF**: Esta medida también sería eficaz, pero en menor medida que la anterior. SPF es un mecanismo de autenticación de correo electrónico que permite a los propietarios de dominios especificar qué servidores están autorizados para enviar correos electrónicos en nombre de su dominio. Si el dominio de origen tiene un registro SPF configurado correctamente y el servidor que está enviando el spam no está autorizado en el registro SPF, es posible que algunos servidores de destino rechacen o marquen los mensajes como spam.
3. **La estafeta de destino es un "open relay"**: Si la estafeta de destino es un "open relay" (un servidor de correo que retransmite mensajes sin autenticación), esto aumentaría la probabilidad de que los mensajes de spam sean entregados con éxito. Los "open relays" son a menudo utilizados por spammers para evadir las medidas de seguridad, ya que permiten el envío de correos electrónicos sin autenticación.
4. **La estafeta de destino requiere autenticación para transmitir mensajes**: Esta medida sería muy eficaz para prevenir el envío de spam. Si la estafeta de destino requiere autenticación para transmitir mensajes, el PC infectado necesitaría credenciales válidas para enviar correos electrónicos a través de ese servidor. Esto limitaría significativamente la capacidad del programa malicioso para enviar spam con éxito.

1. **Esta afirmación es falsa.** La cabecera Host en las peticiones HTTP indica el nombre de dominio al que se está solicitando acceder. No necesariamente tiene que tener la forma xxx.ejemplo.es. Puede ser cualquier subdominio válido dentro del dominio ejemplo.es, incluido alfa.ejemplo.es.

2. **Esta afirmación es correcta.** Un servidor web puede alojar múltiples sitios web, cada uno con su propio certificado SSL/TLS (X.509). Cada certificado puede tener atributos CN (Common Name) diferentes para identificar el dominio al que pertenece.

3. **Esta afirmación es correcta**. Un proxy web directo almacena en caché las respuestas a las solicitudes web, lo que puede acelerar la navegación al proporcionar respuestas más rápidas a las solicitudes repetidas. Además, puede optimizar el ancho de banda al comprimir datos o filtrar contenido no deseado.

4. **Esta afirmación es correcta**. Un proxy web inverso actúa como intermediario entre los clientes web y los servidores web, permitiendo que los servidores web se concentren en procesar solicitudes en lugar de manejar directamente la entrega de contenido a los clientes. Al optimizar la gestión de conexiones y distribuir la carga entre varios servidores, un proxy web inverso puede reducir el tiempo de respuesta percibido por los clientes web.

5. **Esta afirmación es incorrecta**. Un proxy web inverso puede llevar a cabo muchas de sus funciones en sesiones HTTPS, incluyendo el enrutamiento de solicitudes, la gestión de la carga, el balanceo de carga, la compresión de datos, la caché de contenido y la seguridad mediante la inspección SSL/TLS. Sin embargo, algunas funciones, como la inspección profunda de paquetes, pueden ser limitadas en sesiones HTTPS debido a la encriptación de extremo a extremo.