Oposición TAI - tai_2024A_supuesto2

SUPUESTO 2

El Ministerio de Educación, Formación Profesional y Deportes tiene una red asignada en el Plan de Direccionamiento de la AGE 10.9.0.0/16 y ha creado un organismo para la enseñanza online de formadores, OEOF (en adelante nos referiremos en este supuesto sólo como “organismo”), al que le ha correspondido la última de las subredes de las 16 en las que se ha dividido la red ministerial.

El sistema de enseñanza online de formadores se fundamenta en un servidor de formación accesible también desde Internet en la URL https://www.profesores.es. Los servidores de este sistema (web, http, DNS, DHCP, LDAP), se van a instalar con sistema operativo Linux Ubuntu. El portal web está montado usando Apache Tomcat.

El certificado del portal (SSL) estará asociado al dominio profesores.es. Para poder gestionar el correo de los profesores, se ha instalado un servidor de correo con tecnología Postfix.

Los DNS se han instalado usando el software BIND así como la asignación dinámica de direcciones IP mediante DHCP.

Hay un servidor llamado BIBLIOTECA que contiene un compendio de documentos e información de utilidad para los profesores. El acceso está permitido por RDP. En los elementos de configuración está permitido el acceso remoto para todos los usuarios que en el Directorio Activo estén en el Grupo de Profesores. El resto no podrán conectarse. No hay elementos de red que impidan la conexión libre por el puerto RDP 389 a dicho servidor, desde su misma VLAN.

La base de datos de la biblioteca es MySQL.

Además, sobre servidores Ubuntu, se han instalado herramientas de detección de vulnerabilidades (Tenable Nessus y Nmap) y de monitorización de sistemas y de aplicaciones web (Nagios).

Los usuarios de la red (profesores) usan escritorios virtuales.

Los switches para configurar las VLANs son CISCO (usan sistema operativo Cisco IOS).

El CPD principal del organismo tiene un respaldo en un CPD secundario, pero no está configurado como activo-activo y los cambios de los servicios tienen que pasarse manualmente. Tiene redundancia de componentes y de suministro eléctrico y de red. El CPD es TIER III.

Salvo que se indique lo contrario en el enunciado, se supone que usted posee permisos de administrador.

Preguntas

1. ¿Cuántas direcciones hay disponibles para hosts en la subred del organismo?

1. 4094
2. 65534
3. 4096
4. 65536

1. Al arrancar el servidor donde se aloja la web de profesores, aparecen errores en la partición sda8. ¿Qué comando hay que usar para reparar de forma automática los errores en el sistema de ficheros correspondiente, que no ha podido montarse?

1. mount –T /dev/sda8
2. fsck -y /dev/sda8
3. fsck -m /dev/sda8
4. checkdisk /dev/sda8

1. Analizando la seguridad del sistema, surge la duda de si abrir o no el puerto 80 en un servidor web expuesto mediante HTTPS. El Centro Criptológico Nacional recomienda:

1. Exhibir una web estática en el puerto 80 indicando que esa no es la web actual.
2. Cambiar el puerto HTTPS al 8892.

3. Utilizar un analizador de peticiones en las cabeceras HTTP en el puerto 80.
4. Disponer del puerto TCP/80, configurando el servidor web para que lleve a cabo una redirección automática de HTTP a HTTPS.

1. El CPD donde está alojado el sistema tiene una puerta cuyo control de acceso es con tarjeta inteligente y PIN, que sólo conocen los operadores. Hace dos días, se supo que alguien no autorizado había entrado esperando agazapado a que alguien autorizado entrase, pasando detrás de él sin que éste advirtiera que tenía a un intruso detrás. Este incidente de ingeniería social en seguridad física se conoce con el nombre de:

1. Tailgating o piggybacking.
2. Quid pro quo.
3. Pretexto.
4. Disrupción.

1. El organismo tiene, para controlar la seguridad física del CPD, un circuito cerrado de televisión con cámaras que usa una red coaxial y se necesita interconectar esta red a la red local Ethernet para poder monitorizarlas. ¿Con qué dispositivo de red puede hacerlo?

1. Un cortafuegos (firewall).
2. Una pasarela (gateway).
3. Un conmutador (switch).
4. Un repetidor (repeater).

1. En el sistema se utilizan los protocolos DNS y FTP seguro. De acuerdo con el modelo TCP/IP, estos protocolos se diferencian en que:

1. DNS es un protocolo de usuario y FTP es un protocolo de soporte.
2. DNS es siempre un protocolo orientado a la conexión mientras que FTP no.
3. No existe diferencia entre ambos protocolos, ambos son protocolos de soporte.
4. FTP es un protocolo de usuario y DNS es un protocolo de soporte.

1. En un switch Cisco que hay en la organización, se ejecuta el comando “switchport access vlan 1”. Esto permitirá:

1. Asignar un puerto a la VLAN 1.
2. Asignar el puerto 1 del switch a la VLAN donde estamos situados en la consola del switch.

3. Visualizar todos los hosts asignados a la VLAN 1.
4. Asignar todos los hosts conectados a cualquier puerto del switch a la VLAN 1.

1. La base de datos se ha corrompido y además, los usuarios no pueden acceder a la información. Se tiene toda la información de cómo se produjo el incidente y cuál es la persona que lo ha causado y por qué, pero, este incidente, ¿a qué dimensión o dimensiones de la seguridad afecta?

1. A la disponibilidad porque no está accesible la base de datos y la integridad porque el fichero de la base de datos está corrupto.
2. A la confidencialidad porque los datos, una vez dañados, pueden ser accesibles por cualquiera.
3. Sólo a la disponibilidad porque la base de datos está temporalmente fuera de servicio hasta que se repare si es posible el fichero donde se aloja.
4. A la trazabilidad, porque no podremos averiguar lo que ha pasado por mucho que nos esforcemos, la seguridad es así.

1. La red de área local está implementada con Gigabit Ethernet y, al conectar un nuevo dispositivo a la red, en su tarjeta, parpadea una luz de color naranja. ¿A qué puede deberse?

1. A que está mal configurada la VLAN donde está ubicado el dispositivo.
2. A que la tarjeta de red del dispositivo transmite a menor velocidad de la que permite la red.
3. A que la tarjeta de red está estropeada y no hay conexión entre el dispositivo y la red.
4. A que el cable del dispositivo es coaxial y no Ethernet.

1. Nos anuncian que hay una vulnerabilidad que afecta a una determinada versión del kernel de Linux Ubuntu. ¿Con qué comando podemos saber qué versión del kernel tiene nuestro sistema operativo Ubuntu?

1. sudo dpkg -i linux*.deb
2. uname -r
3. uname -o

4. kexec -l

1. Para descargar algunos ficheros del servidor BIBLIOTECA, los administradores están sopesando entre el uso de SFTP y FTPS. Indique, de las siguientes afirmaciones, la INCORRECTA:

1. SFTP usa típicamente el puerto 22 de SSH mientras que FTPS usa el puerto en el que tengamos definido el protocolo SSL/TLS.
2. SFTP usa autenticación con certificado (clave pública) mientras que FTPS usa autenticación con usuario y contraseña.
3. FTPS usa dos puertos, uno para los comandos y otro para descargarse los datos mientras que SFTP usa el mismo puerto para ambas tareas.
4. FTPS no contiene comandos estandarizados para manipular directorios o listar atributos, mientras que SFTP sí.

1. Para la detección de malware complejo y movimiento lateral relacionado con APTs (Advanced Persistent Threats), se ha instalado en los PC de los profesores, la solución del CCN, CLAUDIA. ¿Cómo define el Centro Criptológico Nacional una APT?

1. Es un tipo de ransomware como, por ejemplo, WannaCry, que te cifra los archivos del PC y se requiere la clave de descifrado a cambio del pago de un rescate.
2. Es un ataque de suplantación de identidad de un usuario corriente en un organismo para después mediante escalada de privilegios obtener las credenciales de un alto cargo de la empresa u organización.
3. Es un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país u organización adversaria, por razones que van más allá de las meramente financieras/delictivas o de protesta política.
4. Es un ataque masivo a una organización ocurrido por un fallo que no se había advertido hasta ese momento y, por tanto, no se cuenta con la salvaguarda o parche para prevenirlo.

1. Para mejorar la escalabilidad del sistema, está estudiando implantar una arquitectura de microservicios con Kubernetes. ¿Qué protocolos para servicios pueden utilizarse con Kubernetes?

1. SCTP, TCP (por defecto) y UDP.
2. HTTP (por defecto), HTTPS y FTP.
3. SSH, SFTP (por defecto) y UDP.

4. UDP (por defecto) y TCP.

1. Para poder atender las llamadas de las guardias de sistemas, se han comprado veinte móviles. Su responsable le pide realizar el enrolamiento de estos móviles, pero, ¿en qué consiste esta tarea?

1. Emparejar, en el sistema MDM (Mobile Device Management) de la organización, a cada usuario con su móvil.
2. Dar de alta en una base de datos de administración todos los dispositivos móviles.
3. Insertar la tarjeta SIM correspondiente a cada móvil.
4. Formatear a fábrica todos los dispositivos móviles.

1. Se está instalando la nueva climatización del CPD y se plantea utilizar una toma derivada de la climatización del resto del edificio. ¿Cuál es la razón principal por la que NO se aconseja hacer eso?

1. Porque la humedad recomendada para un CPD es mucho menor que la recomendada para las personas.
2. Porque la temperatura recomendada para un CPD es mucho mayor que la recomendada para las personas.
3. Porque el filtro de impurezas y polvo para las personas es mucho más sensible que lo que se recomienda para un CPD.
4. Porque el aire acondicionado para un CPD siempre debe provenir del techo y para las personas puede provenir lateralmente.

1. Se ha descargado del sitio web del CCN-CERT una herramienta de antimalware y justo debajo aparece un hash de comprobación. ¿Qué tipo de medida de seguridad es este hash en este contexto?

1. Una medida antimalware, pues el hash aplicado al fichero descargado nos sanitiza el fichero y ya se puede usar sin problemas, pues está limpio de malware, lo cual en una herramienta antimalware es altamente necesario.
2. Una medida para asegurar la integridad del fichero de descarga, pues si al calcular nosotros el hash del fichero descargado no coincide con el que nos aparece en la página del CCN, el fichero descargado no sería válido para su uso.
3. El hash es la firma del CCN como autoridad de certificación de productos que garantiza que el software descargado es apto para ser usado en sistemas categorizados como de nivel ALTO o incluso en sistemas clasificados como reservado nacional.
4. El hash es la firma del CCN de la página web donde se presenta la herramienta que estamos intentando descargar y es una medida

para evitar que los hackers puedan manipular la página y subir otro fichero en vez del que se pretende descargar.

1. Se ha implantado una solución VoIP que usa el protocolo SIP pero, al establecer sesiones con usuarios de fuera del organismo, la llamada se corta o congela y después, se restablece. Este problema no sucede en sesiones entre usuarios internos del organismo, ¿por qué puede ser?

1. Se están usando incorrectamente los códecs.
2. La salida a Internet está empleando NAT.
3. El tráfico entre origen y destino está interceptado en el cortafuegos de Internet.
4. La CPU del ordenador es insuficiente y provoca estos problemas.

1. Se ha instalado un servidor de correo con Postfix y se está decidiendo si utilizar POP3 o IMAP en los clientes de correo. ¿Cuál de las siguientes opciones es INCORRECTA?

1. Con IMAP, los mensajes se almacenan en un servidor remoto y los usuarios pueden iniciar sesión en varios clientes de correo electrónico y leer los mismos mensajes.
2. POP3 solo admite la sincronización de correo unidireccional, lo que solo permite a los usuarios descargar correos electrónicos desde un servidor a un cliente.
3. Con IMAP, el correo enviado y recibido se almacena en el servidor hasta que el usuario lo elimina permanentemente.
4. Con POP3, si los usuarios organizan sus correos electrónicos en un dispositivo mediante carpetas, ya no tendrán que hacerlo en el resto de dispositivos porque se replica la organización en carpetas.

1. Se necesita saber los usuarios que acceden a la base de datos de la biblioteca y desde qué host o IP. Para averiguarlo, en la consola de administración de la base de datos, ejecutará el comando:

1. SELECT * FROM all_users
2. mysql> SELECT user FROM mysql.user
3. mysql> SELECT user,host FROM mysql.user

4. sudo mysql -u root -p

1. Se quiere aplicar políticas de seguridad al grupo de usuarios Profesores utilizando Directorio Activo y GPOs. Una buena práctica es definir primero:

1. Una Unidad Organizativa (OU) para el grupo de usuarios Profesores.
2. Las ACLs (Access Control Lists) que tendrán las GPO del grupo de usuarios Profesores.
3. Un nuevo bosque de Directorio Activo.
4. Relaciones de confianza entre el Directorio Activo actual y el dominio de seguridad del grupo de usuarios Profesores.

Preguntas de reserva

1. Como administrador de correo, quiere cambiar el mensaje HELO que aparece cuando se establecen conexiones al servidor SMTP. Actualmente aparece el nombre del servidor, pero quiere que muestre “CORREOBIBLIOTECA” y además, que el cambio se aplique en todos los servidores SMTP que existan, no solo en aquel en el que está trabajando. ¿Cómo lo haría?

1. Editando el parámetro $client en el fichero /etc/postfix/main.cf y reiniciando posteriormente el servidor Postfix.
2. Accediendo al servidor SMTP y ejecutando EHLO -name CORREOBIBLIOTECA en la consola.
3. Editando el parámetro smtp_helo en el fichero /etc/postfix/master.cf y reiniciando posteriormente el servidor Postfix.
4. Editando el parámetro $helo_name en /etc/postfix/main.cf y reiniciando posteriormente el servidor Postfix.

1. Como no hay suficientes tomas Ethernet en la zona física donde están los profesores, se va a instalar una red WiFi con protocolo WPA3-Enterprise. En este caso, para acceder a la red WiFi habrá que utilizar:

1. Una contraseña de 64 bits.
2. Una contraseña de 128 bits.
3. Un servidor RADIUS o cualquier solución que permita EAP-TLS.
4. Una contraseña de 192 bits usando el algoritmo GMCP-256.

1. En la base de datos MySQL de Profesores, nos piden que añadamos una tabla de los profesores para el curso de INGLES BASICO, que se llamará “ProfesoresIngles” con sus nombres y

apellidos. Para ello, y tras acceder como root a MYSQL, ingresaremos el comando:

1. CREATE TABLE ProfesoresIngles (id INT NOT NULL PRIMARY KEY AUTO_INCREMENT, nombre VARCHAR(30), apellido1 VARCHAR(30), apellido2 VARCHAR(30));
2. CREATE TABLE ProfesoresIngles KEY id, nombre, apellidos;
3. CREAR TABLA ProfesoresIngles KEY apellidos, nombre;
4. CREATE TABLE ProfesoresIngles (nombre, apellido);

1. Ha instalado el servicio Nagios para monitorizar los servidores y servicios en su sistema y quiere monitorizar, además, la URL de profesores (https://profesores.es), pero antes quiere comprobar que este servicio está configurado correctamente. Para ello, utilizará el comando:

1. nagios –v /usr/local/nagios/etc/nagios.cfg
2. /mnt/nagios –check
3. systemctl status nagios
4. https://profesores.es nagios

1. Se ha instalado un servidor web con HTTPS y certificado SSL de servidor para proteger la conexión entre los clientes y el servidor, para lo cual la conexión usará TLS. Según las recomendaciones del Centro Criptológico Nacional, ¿cuál es la versión mínima y la recomendada a usar en TLS?

1. La versión mínima aceptable es la 1.1 y se recomienda usar esa misma versión 1.1
2. La versión mínima aceptable es la 1.0 y se recomienda usar 1.1
3. La versión mínima aceptable es la 1.2 y se recomienda usar la 1.3
4. La versión mínima aceptable es la 1.1 y se recomienda usar la 1.3