SUPUESTO PRÁCTICO 1. (Puntuación máxima 15,5)

Es un objetivo de este año de la Sindicatura de Comptes poder certificarse en el nivel medio del Esquema Nacional de Seguridad (ENS) para todos los sistemas de información. Desde el departamento de informática se quieren realizar los trabajos necesarios que permitan llegar en el estado de madurez necesario para poder obtener dicha certificación por parte de la empresa que resulte adjudicataria de la certificación, con el alcance especificado (todos los sistemas de información).

Para ello, es necesario analizar los sistemas de información, identificar carencias en estos y, posteriormente, realizar las actuaciones correspondientes para su subsanación.

En este supuesto práctico, teniendo en cuenta que en la Sindicatura se dispone de entornos Microsoft Windows y Linux, se pide responder a las siguientes preguntas:

1. En los sistemas Windows ¿qué herramienta del CCN-CERT permite a las Administraciones públicas analizar las características de seguridad técnica definidas en el ENS para los sistemas de nivel medio? ¿Y para determinados sistemas Linux? (0,5 puntos)

2. En caso de que los sistemas fueran de nivel alto, para los sistemas Windows ¿qué herramienta se debería utilizar para el mismo objetivo de la pregunta anterior? (0,5 puntos)

3. ¿En qué modalidades se puede desplegar la herramienta a que nos hemos referido en la pregunta 1? (1 punto)

4. ¿Qué tipos de informes se generan con esta herramienta? Describa cada uno de ellos brevemente. (1 punto)

5. Indique dos elementos de información que pueden ser objeto de recomendación en el informe más detallado de entre los que se obtienen como resultado del análisis con la herramienta mencionada en las preguntas anteriores. Indique en qué informe aparecen dichos elementos de información. (1 punto)

6. ¿Con qué otros recursos del CCN-CERT contaría para ayudarte en estas tareas? (1 punto)

7. ¿Qué herramienta del entorno Microsoft Windows se puede utilizar para comparar nuestra configuración de seguridad frente a configuraciones de seguridad estándar verificadas? (1 punto)

8. Una de las deficiencias detectadas en un análisis de seguridad ha sido que todos los ordenadores personales de la red tenían la misma contraseña de administrador local y sin caducidad. ¿Cuál será la forma óptima y nativa de solventar esta deficiencia? ¿Cuál sería su funcionamiento básico? (1,25 punto)

9. Antes de usar esta herramienta, el esquema de Windows Server Active Directory debe actualizarse. ¿Qué comando debe utilizarse? (1,25 punto)

10. Utilizando las funcionalidades del propio sistema Windows ¿Cómo podemos comprobar que la contraseña se ha actualizado correctamente en Windows Server Active Directory? (1 punto)

11. ¿Sobre qué elementos del directorio activo de Microsoft Windows se aplican las políticas de grupo (GPO) y a qué objetos afectan? (1 punto)

12. ¿Cuál sería el orden correcto del procesamiento de las GPO suponiendo que estén configuradas todas? (1 punto)

13. ¿Qué ocurre cuando dos GPO establecen una directiva en sentidos contrarios? (1 punto)

14. En el equipo SC0245, del usuario sgonzalez, se ha detectado que no se ha aplicado una directiva. ¿Cómo se puede forzar a la ejecución de la GPO sin tener que esperar a que se aplique según se haya establecido la periodicidad de la misma desde la terminal de un administrador? Se quieren aplicar todas las configuraciones de directiva aplicables en una única orden. (1 punto)

15. ¿Qué comando permitiría al administrador extraer información de forma remota de qué directivas se están aplicando en el equipo SC0245, cuya IP es 192.168.1.11? Se quiere guardar la salida en el fichero gpoSC0245.txt. (1 punto)

16. Con respecto a las GPO, ¿qué son los ficheros .admx? (1 punto)

SUPUESTO PRÁCTICO 2 (PUNTUACIÓN MÁXIMA 15,5 PUNTOS)

PLANTEAMIENTO

Una organización pública dispone de servidores virtualizados Windows (2016 y 2019) y Linux (Ubuntu y CentOS), sobre un sistema de virtualización VMWare. Por cuestiones económicas, se ha desplegado un sistema en cluster de virtualización ProxMox VE, basado en hipervisor KVM, y se está planificando la migración de esos servidores virtualizados al nuevo entorno.

Los servidores virtuales Linux tienen volúmenes de almacenamiento LVM2, con sistemas de ficheros Ext4 y XFS. Los servidores virtuales Windows manejan sistemas de ficheros NTFS.

Desde un punto de vista de conectividad de red, la organización dispone de una red segmentada en diferentes VLANs que están distribuidas y gestionadas sobre la electrónica de red. Sin embargo, se ha detectado que es conveniente realizar una mejor segmentación de dicha red para separar ciertos tráficos. En la actualidad, hay tres redes VLAN: LAN, DMZ y WIFI, que cursan, respectivamente, el tráfico de PC corporativos y servidores internos (LAN), servidores expuestos a Internet (DMZ), y PCs conectados a la red inalámbrica de la organización, corporativos o no (WIFI).

Todo el tráfico de esas redes pasa por un cluster de cortafuegos, que conecta además la organización a Internet, y que sirve de terminador de túneles VPN para el acceso remoto seguro de los usuarios de la organización a recursos internos de la misma. También sobre esa infraestructura de cortafuegos se conectan las cinco sedes de la organización, en una topología en estrella, cuyo centro es la Sede Principal.

PREGUNTAS

1. ¿En qué formato estándar se deberían exportar las máquinas virtuales de VMWare para poder ser importadas en ProxMox VE u otros sistemas de virtualización? (0,5 puntos)

2. ¿Cuál es el principal requisito para que se pueda realizar una migración sin parada de una máquina virtual entre dos nodos de un cluster de virtualización, suponiendo que existe comunicación entre ambos? (0,5 puntos)

3. En una de las máquinas virtuales Ubuntu Linux se ha detectado que las aplicaciones que en él residen van más lentas de lo normal, y el monitor de la virtualización nos indica que se está haciendo un uso muy alto de la vCPU. ¿Cómo se podría averiguar qué proceso o

procesos de la máquina virtual están provocando ese uso excesivo de CPU? (0,5 puntos)

4. En otra de las máquinas virtuales Ubuntu Linux se ha detectado que va a hacer falta espacio extra en un volumen donde se almacenan datos de una aplicación. Tras planificar una parada par ello, y parar la aplicación, se pretende hacer crecer el volumen lógico LVM, denominado cl-root, del grupo LVM cl-grupo, donde residen esos datos. Para ello, se ha añadido un volumen en la virtualización, que se muestra como /dev/sdd en esa máquina virtual. Indique, de forma ordenada, los comandos que ejecutaría para extender el volumen lógico LVM cl-root y el sistema de ficheros en él almacenado, con todo el espacio agregado a la máquina virtual con /dev/sdd y dejarlo todo listo para poder arrancar la aplicación con más espacio disponible. Comente de forma breve qué hace en cada paso. (2 puntos)

5. En el replanteamiento de la segmentación de la red, teniendo en cuenta la información aportada en el caso, las buenas prácticas en gestión de redes, y los requisitos al respecto que impone el Anexo II del Esquema Nacional de Seguridad en su nivel Medio, indique qué VLANs como mínimo deberían tenerse en la red del organismo, y qué tráfico debería cursarse en cada una de ellas. (1,5 puntos)

6. De las VLAN que haya definido en el ejercicio anterior, establezca una propuesta de filtrado de tráfico en el cortafuegos, pensando en la naturaleza de dicho tráfico y la mejora de la seguridad, mediante una tabla, que indique si el tráfico con origen en la VLAN A puede cursarse o no a la VLAN B, indicando uno de estos tres valores en cada celda de la tabla:

- P: permitido, pero sujeto a otras posibles reglas de filtrado más granulares
- R: permite sólo las respuestas a peticiones de VLAN B
- D: denegado incondicionalmente

Indique solamente con estos valores el tráfico que pasará por el firewall según su propuesta, y justifique los aspectos que desee resaltar de la misma (2,5 puntos).

7. Para empezar con la configuración de las reglas de cortafuegos, se plantean definir los tráficos siguientes:

- Los definidos en la tabla del ejercicio anterior.
- Acceso permitido a consultas de DNS desde las VLANs LAN, WIFI, DMZ y GESTION. Los servidores de DNS se encuentran en la VLAN SERVER (se pueden identificar como DNSSRV1 y DNSSRV2).

Defina óptimamente las reglas tomando como modelo la tabla siguiente, y teniendo en cuenta que por políticas del fabricante del cortafuegos, siempre se acepta el tráfico de

respuesta a un tráfico iniciado desde una regla de aceptación:

N.º orden	Protocolo	Origen	Puerto	Destino	Puerto	Acción

(3 puntos)

8. Indique qué regla definiría, y entre qué dos reglas de la tabla que ha construido en el ejercicio anterior la colocaría, para que se denegara el tráfico generado por los comandos ping hacia la red de GESTION. (0,5 puntos)

9. La organización estima que, una vez realizada correctamente la segmentación de sus redes, la VLAN LAN tendrá un máximo de 200 equipos, y la VLAN WIFI puede llegar a tener 350 equipos conectados. Si un organismo jerárquicamente superior ha asignado a la organización las redes 192.168.10.0/24, 192.168.11.0/24 y 192.168.12.0/24, indique cuál será el direccionamiento asignado a cada VLAN y por qué. (0,5 puntos)

10. Igualmente, la organización tiene asignado un direccionamiento IP 192.168.13.0/24, que ha de utilizarse para direccionar los dispositivos de otras cuatro redes, en cuatro ubicaciones diferenciadas, que denominaremos genéricamente RED1, RED2, RED3 y RED4, y que han de poder direccionar, respectivamente 70, 35, 22 y 18 dispositivos. Indique una posible propuesta de direccionamiento para cada una de esas tres redes, rellenando la tabla siguiente:

Red	Direccionamiento	N.º máximo de dispositivos direccionables	Primera dirección utilizable para un dispositivo	Última dirección utilizable para un dispositivo
RED1				
RED2				
RED3				
RED4				

(1 punto)

11. Las redes mencionadas en el ejercicio anterior se van a utilizar para direccionar los dispositivos de cuatro pequeñas sedes de la organización, que se encuentran conectadas a través de Internet hacia una sede central, con una topología en estrella. Indique dos requisitos que han de cumplir los dispositivos que interconecten esas sedes y el mecanismo mediante el cual se establece una interconexión segura. (0,5 puntos)

12. De acuerdo al Anexo II del Esquema Nacional de Seguridad, se ha detectado que el mecanismo de autenticación con usuario y contraseña para la VPN no es suficiente. ¿Qué mecanismo de autenticación propondría para cumplir con lo establecido para un nivel Medio del ENS, y que no suponga una excesiva carga administrativa o económica para la organización? Indique un ejemplo de uso. (1 punto)

13. Se ha desplegado en una máquina virtual un servicio web. Para cumplir con lo establecido en el Esquema Nacional de Seguridad, ¿qué herramienta utilizaría en primer lugar para analizar la seguridad de dicha máquina virtual como uno de los pasos previos a su paso a producción? (0,5 puntos)

14. En un sistema operativo Linux, salvo configuración expresa en contra, ¿dónde se se guardan las credenciales de los usuarios del sistema? (0,5 puntos)

15. ¿Qué comando Linux nos permite comprobar el tamaño libre de los discos del sistema? (0,5 puntos)

16. Al conectar a la consola de una máquina virtual Ubuntu Linux, el sistema nos advierte de que hay actualizaciones de seguridad pendientes de aplicar. ¿Qué comando(s) lanzaría para actualizar al máximo la máquina? (0,5 puntos)

17. ¿Qué puertos se deben abrir en el cortafuegos para poder ofrecer los siguientes servicios (pop, imap, smtp, ssh, https)? (0,5 puntos)