Prepara tu examen de BRS

Introducción

Cada centro, cada año y cada docente, puede plantear al alumnado un modelo de examen concreto que, a su criterio, pueda servir como una correcta evaluación del módulo.

Para ayudar a preparar las evaluaciones, he pensado que podría ser de ayuda crear un archivo único para cada módulo, que pueda crecer cada año con el feedback y apoyo de la comunidad, con cuestionarios de todo tipo, con solucionario o solo los enunciados, pues la intención primera es poder ofrecer una idea de lo que podemos encontrarnos a la hora de una evaluación, poder aprender con ello, y no algo que una persona acabe memorizando, y esperando, sin comprender ni ahondar en la materia, que aparezca mágicamente en el examen.

Este documento, por tanto, no pretende ser una guía única y veraz de exámenes pasados o futuros, pero si una fuente de información sobre la que basar vuestros estudios.

Posibles modelos.

Modelo 1.

Ejemplo para preparación.

Trabajas para una empresa de consultoría de ciberseguridad y habéis sido contratados por la empresa ElectroElf, que se dedica a la venta online de productos electrónicos. Esta empresa ha experimentado un crecimiento significativo en los últimos años y ha aumentado su presencia en el mercado, lo que la convierte en un objetivo atractivo para la ciberdelincuencia.

Nuestro objetivo es decidir la nueva infraestructura de la empresa y proponer medidas de seguridad que puedan implementarse para mejorar la protección de sus sistemas y datos. Cuenta con una red de equipos y servidores que almacenan información sensible, como datos de clientes y proveedores, información financiera y de ventas, entre otros.

En el pasado, ha sufrido algunos incidentes de seguridad, como ataques de phishing y malware, que han afectado a algunos de sus empleados y sistemas. Además, no cuentan con un plan de seguridad sólido y las políticas de seguridad son poco claras y no se cumplen de manera consistente.

Teniendo en cuenta que los dispositivos de red cableada con los que cuentan son:

Dispositivo	**Función**
Router	Conexión a Internet y servicio DHCP
Cortafuegos con tres adaptadores de red	Protección y aplicación de reglas de seguridad de las diferentes redes
Switch 1	Punto de conexión entre equipos
Switch 2	Punto de conexión entre equipos

Y que los servidores físicos que tienen actualmente son:

Servidor	**Función**
Servidor de correo electrónico	Comunicación interna y externa
Servidor de almacenamiento de datos	Información sobre los clientes solamente accesible para trabajadores
Servidor web	Página web de comercio electrónico

1. (Puntuación: 2). Elabora un diagrama lógico en el que indiques cómo conectas los dispositivos de red con los servidores para que la infraestructura sea lo más segura posible.

Responde a las siguientes preguntas que te realiza el CTO de la empresa, eligiendo siempre la opción más segura posible:

2. (Puntuación: 1. Resta 1/3 puntos una respuesta incorrecta). Si optamos por permitir el teletrabajo para el administrador de sistemas, ¿Qué opción sería la mejor?

a) Instalar y configurar un servicio VPN en un servidor y abrir el puerto necesario en el router para el acceso desde Internet.
b) Instalar y configurar un servicio SSH en los servidores y abrir los puertos necesarios en el router para el acceso desde Internet.
c) Instalar y configurar un servicio de escritorio remoto en todos los equipos y abrir los puertos necesarios en el router para el acceso desde Internet.
d) Configurar un servidor interno que tenga acceso remoto a todos los equipos de la red empresarial y que el administrador de sistemas se conecte a través de Internet usando Telnet, abriendo el puerto necesario.

3. (Puntuación: 1. Resta 1/3 puntos una respuesta incorrecta). Si instalamos en la red interna algunos puntos de acceso para permitir a los empleados la conexión inalámbrica. ¿Qué protocolo tendríamos que intentar utilizar?

a) RADIUS.
b) TACACS.
c) DIAMETER.
d) NAC.

4. (Puntuación: 1. Resta 1/3 puntos una respuesta incorrecta). ¿Cuál de las siguientes herramientas podríamos utilizar como SIEM?

a) Logstash.
b) Splunk.
c) AppArmor.
d) EternalBlue.

Es el momento de hacer una propuesta concreta de seguridad frente a determinados aspectos. Lo harás de forma guiada contestando con respuestas cortas a las siguientes preguntas:

5. (Puntuación: 0,5). En el pasado, la empresa ha tenido algunos problemas provocados por empleados descontentos. ¿Qué paradigma de seguridad les sugieres implementar?

6. (Puntuación: 1). ¿Qué estrategia global les recomiendas para las copias de seguridad?

7. (Puntuación: 1). Indica una medida de seguridad que les pueda ser útil frente a ataques Syn Flood (DDoS).

8. (Puntuación: 1). Elabora una propuesta de uso de 2FA para el acceso a las cuentas empresariales.

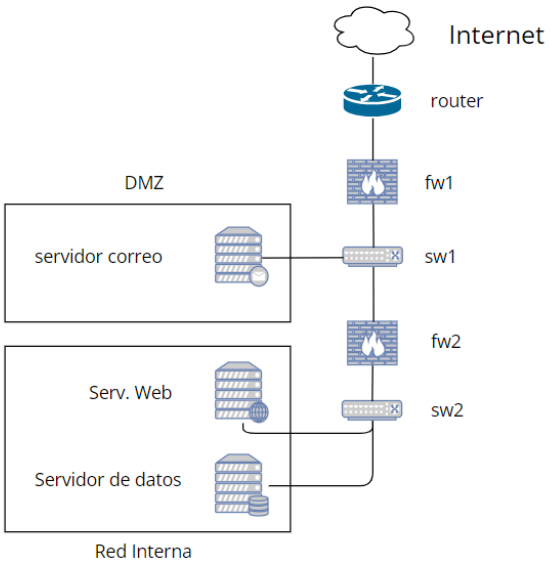
9. (Puntuación: 1). Indica una forma de mitigar la presencia de Shadow IT en la empresa.

10. (Puntuación: 0,5). ¿Qué tipo de herramienta deben instalar en los equipos de los empleados para detectar actividades sospechosas?

Modelo 2.

1. Diagrama de red

- ✓ Dispositivo
  - Router: conexión a Internet y servicio DACP
  - Cortafuegos 1: con dos adaptadores de red: protección y separación de las diferentes redes
  - Cortafuegos 2: con dos adaptadores de red: protección y separación de las diferentes redes
  - Switch 1: punto de conexión entre equipos
  - Switch 2: punto de conexión entre equipos
- ✓ Servidor
  - De correo electrónico: comunicación interna y externa
  - De almacenamiento de datos: información sobre pacientes, médicos y proveedores
  - Web: portal web para la gestión de historiales médicos, con una BBDD más limitada a los datos necesarios para su funcionamiento.



Test

2. Implementar DLP, ¿a qué os referís?

a. Conjunto de herramientas que tiene como finalidad prevenir las fugas de información.
b. Conjunto de soluciones antimalware con medidas o funciones reactivas.
c. Técnica de cifrado de datos asimétricos.
d. Solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones de negocio.
ANSWER: A

3. Implementación de una infraestructura PKI, ¿cuál es el principal propósito de esta infraestructura?

a. Monitorear el tráfico de red.
b. Cifrar y firmar datos.
c. Proporcionar una red privada y segura sobre una red pública.
d. Aumentar la velocidad de internet.
ANSWER: B

4. Se desea que se realice una gestión óptima de las amenazas y automatizar las posibles operaciones de seguridad. ¿Qué deberíamos recomendar implementar como solución?

a. SIEM
b. SOAR
c. VPN
d. IDS
ANSWER: C

Preguntas cortas

5. ¿Cuál es el servicio que deberían implementar para que los trabajadores que no se encuentren físicamente en la oficina puedan acceder a la información sensible necesaria para desempeñar su trabajo? ANSWER: VPN*.

6. ¿Qué proyecto de código abierto deberían revisar para proteger la aplicación web frente a los tipos más comunes de vulnerabilidades? ANSWER: OWASP*.

7. Desde la sensibilidad de los datos con los que trabaja, ¿qué deben implementar para garantizar que los datos confidenciales de la empresa no se pierdan, se utilicen de forma inapropiada o puedan acceder a ellos usuarios no autorizados? ANSWER: DLP*.

8. ¿Qué modelo de movilidad empresarial o política referente al uso de dispositivos móviles en la empresa deberían implementar para maximizar la seguridad y minimizar la fuga de información? ANSWER: MDM*.

9. ¿Qué tipo de firewall les recomendarías implementar para que tenga funcionalidades de otros dispositivos de seguridad como IPS, IDS o WAI? ANSWER: NGFW*.

10. Mediante que herramientas podríamos proporcionar controles y gestionar las aplicaciones en la nube de la empresa. ANSWER: CASB*.

*FALTA DESARROLLAR ESAS RESPUESTAS