¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % **Calificación del último envío** 100 % **Para Aprobar** 80 % o más

Ir al siguiente elemento

1. ¿Cuáles son los objetivos de realizar una actualización de parches para el reforzamiento de la seguridad? Selecciona todas las opciones que correspondan. **1 / 1 punto**

- [ ] Evitar que agentes de amenaza inunden una red.
- [x] Actualizar un sistema operativo a la última versión del software.

Correcto

- [ ] Requerir que un/a usuario/a verifique su identidad para acceder a un sistema o red.
- [x] Corregir vulnerabilidades de seguridad conocidas en una red o en servicios.

Correcto

2. ¿Cuál es la relación entre el reforzamiento de la seguridad y una superficie de ataque? **1 / 1 punto**

- ( ) El reforzamiento de la seguridad expande la superficie de ataque.
- ( ) El reforzamiento de la seguridad aumenta la superficie de ataque.
- ( ) El reforzamiento de la seguridad elimina permanentemente la superficie de ataque.
- (•) El reforzamiento de la seguridad disminuye la superficie de ataque.

Correcto

3. Completa el espacio en blanco: Exigir a los/las empleados/as que apaguen sus dispositivos personales mientras están en áreas seguras es un ejemplo de una práctica de reforzamiento de la seguridad _____. **1 / 1 punto**

- ( ) centrada en la red
- ( ) virtual
- ( ) basada en la nube
- (•) física

Correcto

4. El equipo ejecutivo de una empresa aprueba una propuesta del/de la director/a de seguridad. La propuesta consiste en que profesionales de seguridad simulen un ataque a los sistemas de la empresa para identificar vulnerabilidades. ¿Qué describe este escenario? **1 / 1 punto**

- ( ) Detección de paquetes
- ( ) Ping de la muerte
- (•) Prueba de penetración
- ( ) Un ataque de denegación de servicio distribuido (DDoS)

Correcto

5. ¿Cuáles de las siguientes son tareas de reforzamiento del SO? Selecciona tres respuestas. **1 / 1 punto**

- [x] Implementar la autenticación de múltiples factores

Correcto

- [x] Ejecutar copias de seguridad programadas regularmente

Correcto

- [ ] Configurar un firewall
- [x] Usar estándares de cifrado seguro

Correcto

6. Un/a analista de seguridad advierte algo inusual que afecta al sistema operativo (SO) de su empresa. Para confirmar que no se han realizado cambios en el sistema, el/la analista compara la configuración actual con la documentación existente sobre el SO. ¿Qué describe este escenario? **1 / 1 punto**

- (•) Comprobación de la línea base de configuración
- ( ) Gestión responsable de las aplicaciones
- ( ) Actualización de la interfaz entre el hardware de la computadora y el usuario
- ( ) Verificación de la identidad del usuario al acceder a un SO

Correcto

7. Completa el espacio en blanco: La medida de seguridad de autenticación de múltiples factores (MFA) requiere que un/a usuario/a verifique su identidad _____ antes de acceder a un sistema o red. **1 / 1 punto**

- ( ) en 60 segundos
- (•) de dos o más formas
- ( ) todos los días
- ( ) al menos una vez

Correcto

8. ¿De qué manera se podría utilizar el filtrado de puertos para proteger una red de un ataque? **1 / 1 punto**

- ( ) Para ayudar a las/los analistas a inspeccionar, analizar y reaccionar ante los eventos de seguridad en función de su prioridad
- (•) Para deshabilitar los puertos no utilizados con el fin de reducir la superficie de ataque
- ( ) Para crear subredes aisladas para diferentes departamentos en una organización
- ( ) Para aumentar la superficie de ataque en una red

Correcto

9. Un equipo de seguridad considera la mejor manera de manejar las diferentes zonas de seguridad dentro de su red. Prioriza la protección de la zona restringida al separarla del resto de la red y garantizar que tenga estándares de cifrado mucho más altos. ¿Qué describe este escenario? **1 / 1 punto**

- (•) Segmentación de red
- ( ) Prueba de penetración
- ( ) Reforzamiento de la nube
- ( ) Actualización de parches

Correcto

10. ¿Cómo puede un/a profesional de seguridad confirmar que no se han producido cambios no verificados dentro de un servidor en la nube? **1 / 1 punto**

- ( ) Realiza una prueba de penetración
- ( ) Utiliza el filtrado de puertos para bloquear o permitir ciertas actualizaciones
- ( ) Establece una autenticación de múltiples factores (MFA)
- (•) Compara la imagen de línea base del servidor con los datos de los servidores en la nube

Correcto