1er parcial seguridad

1. Según la definición de “Daño” seleccione la respuesta correcta:
   A. Debe ser cuantificable
   B. Todas las respuestas son correctas
   C. Ocurre solo cuando se inhabilita el sistema de forma completa
   D. Se debe expresar en probabilidad de ocurrencia

2. ¿Cuáles de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS?
   A. Recolección – Identificación – Clasificación
   B. Recolección – Análisis – Respuesta
   C. Ninguna de estas opciones
   D. Filtrado – Identificación – Acción

3. La seguridad de la información comprende:
   A. Plan director / Configuración Segura / Auditoria de Eventos
   B. Normativas / Técnicas de Protección / Plan Director
   C. Análisis de Riesgo / Normativas / Plan Director
   D. Análisis de Riesgo / Auditoria de Eventos / Normativas

4. ¿Cuál de los siguientes tipos NO corresponde a la lista OWASP de 10 Ataques mas frecuentes?
   A. Inyección
   B. Control de accesos sin contraseñas seguras
   C. Fallas en el Registro y Monitores
   D. Perdida de autenticación y gestión de sesiones.

5. ¿Cómo se denomina a la zona ubicada entre la red interna y la externa donde habitualmente se ubican a los servidores de la empresa (WEB, DB, FTP, Etc.)?
   A. B2B
   B. LBA
   C. DMZ
   D. Router

6. ¿Qué es un firewall?
   A. Un dispositivo de antivirus de red
   B. Un dispositivo que permite la autenticación en aplicaciones
   C. Un dispositivo que permite bloquear o filtrar el acceso entre dos redes usualmente una privada y otra externa.

7. ¿Cuál de las siguientes tecnologías NO puede ser utilizada en un ataque de inyección?
   A. SQL
   B. Ninguna de estas opciones
   C. LDAP
   D. X-Patch

8. Indique a que termino se asocia la siguiente definición: “[…] es la propiedad que busca mantener los datos libres de modificaciones autorizadas”
   A. Confidencialidad
   B. Integridad
   C. Consistencia
   D. Disponibilidad

9. ¿Cuál es el conjunto de estándares que nos permite asignar a las vulnerabilidades una valoración numérica entre 0.0 y 10.0?
   A. CVE
   B. TopTen
   C. CVSS
   D. CWE

10. Indique el tipo de ataque correspondiente a la siguiente definición: “ocurre cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.”
    A. Perdida de autenticación y gestión de sesiones.
    B. Inyección
    C. Falsificación de peticiones en sitios cruzados (CSRF)
    D. Referencia directa insegura a objetos