1 - ¿A qué tipo de equipo se está refiriendo la siguiente definición?

“Analiza el tráfico de la red para tratar de detectar patrones sospechosos que indiquen ataques o intenciones de ataques contra algún recurso. Una vez identificados, puede tomar ciertas medidas contra ese tipo de tráfico, como generar alertas o inclusive bloquear o descartar el tráfico que viene de ese origen.”

A – Statefulls

B – HoneyPots

C – HoneyNets

D – IDS

2 - ¿A qué ataque del OWASP Top-Ten se refiere la siguiente definición: “El atacante puede ejecutar secuencias de comandos en el navegador de la víctima…”?

A – Secuencia de Comandos en Sitios Cruzados (XSS)

B – Falsificación de Peticiones en Sitios Cruzados (CSRF)

C – Ausencia de Control de Acceso a Funciones

D – Referencia Directa Insegura a Objetos

3 – 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 a datos no autorizados.”

A – Perdida de autenticación y gestión de sesiones

B – Falsificación de peticiones en sitios cruzados (CSRF)

C – Referencia directa insegura a objetos

D – Inyección

4 – Seleccione el tipo de ataque correspondiente a la siguiente definición: “es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.”

A – Inyección

B – Perdida de autenticación

C – Tampering

D – Denegación de Servicio

5 - ¿Cuál de los siguientes factores no es evaluado por la OWASP para determinar los riesgos incluidos en el proyecto Top-Ten?

A – Impacto en el Negocio

B – Impacto Técnico

C – Vectores de Ataque

D – Detectabilidad de Debilidades

6 - ¿Cuál de las siguientes tecnologías no puede ser utilizada en un ataque de Inyección?

A – SQL

B – LDAP

C - Ninguna

D – X-Path

7 - ¿Cuál es la principal función de un comprobador de integridad?

A – Identificar los cambios realizados en los archivos del sistema

B – Notificar vía email sobre cambios en el sistema de archivos

C – Identificar al usuario que ha introducido cambios en el sistema de archivos

D – Identificar archivos que han sido alterados en el sistema de archivos

8 - ¿Cuál de los siguientes elementos corresponde a una Modalidad de Acceso a la información en Seguridad Lógica?

A – Todas las opciones

B – Borrado

C – Escritura

D – Lectura

E – Ejecución

9 - ¿Cuál de estos elementos corresponde a la siguiente definición?:

“Se trata de un dispositivo que analiza el trafico web (entre el servidor web y la WAN), los datos recibidos por parte del usuario y protege de diferentes ataques”

A – Firewall Personal

B – WAF

C – Layer 3 Firewall

D – IDS

10 - ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID?

A – Identificación

B – Ninguno

C – Confidencialidad

D – Disponibilidad

11 - Explique el ataque por Injection comparándolo y asociándolo con el de XSS.

Adicionalmente indique que medidas se recomiendan para proteger a una aplicación de este ataque

12 – Desarrolle la definición y función de un IDS, explique sus diferencias con un IPS y un Firewall.