1 - ¿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 – Ausencia de Control de Acceso a Funciones

C – Falsificación de Peticiones en Sitios Cruzados (CSRF)

D – Referencia Directa Insegura a Objetos

2 - ¿Cuál de estas tecnologías es considerada generadora de riesgo por ser ejecutada en el cliente?

A – Java Applet

B – ActiveX

C – JavaScript

D – Todas las respuestas

3 - ¿Cuáles de los siguientes puntos NO corresponde a un tipo de vulnerabilidad?

A – Debidas al uso

B – Debidas al diseño

C – Debidas a la implementación

D – Ninguna de las anteriores

4 – ¿Cuáles de estas afirmaciones es verdadera en la relación a los Firewalls?

A – No protege de accesos no autorizados

B – No protege de ataques internos

C – Todas las anteriores

D – No protege de todos los ataques dañinos

5 - ¿Cuál de los siguientes puntos no es un atributo del protocolo TCP?

A – No es orientado a conexión

B – Corre sobre IP

C – Cada paquete tiene un numero de secuencia y un flag

D – Un paquete tiene un numero de origen y destino

6 - ¿Qué se entiende por tampering?

A – Es una técnica para redireccionar al usuario hacia otro servidor

B – Es un ataque de alteración de datos no autorizados

C – Ninguna respuesta es correcta

D – Es una vulnerabilidad que afecta al código JavaScript

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

A – Vectores de Ataque

B – Detectabilidad de Debilidades

C – Impacto Técnico

D – Impacto en el Negocio

8 - ¿Qué es un bugtraq?

A – Ninguna de las opciones es correcta

B – Es una lista de notificación sobre vulnerabilidades encontradas en software y hardware

C – Es una variante de virus o troyano

D – Es un software diseñado para buscar vulnerabilidades

9 - ¿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 – DMZ

B – B2B

C – Router

D – LBA

10 - ¿Qué es un firewall?

A – Un dispositivo que permite bloquear o filtrar el acceso entre dos redes; usualmente una privada y otra externa

B – Un dispositivo de antivirus de red

C – Una librería de software que permite asegurar una aplicación web

D – Un dispositivo que permite la autenticación en aplicaciones

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

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

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

C – Identificar los cambios realizados en los archivos del sistema

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

12 - ¿Qué se entiende por tampering?

A – Es un ataque de alteración de datos no autorizados

B – Es una vulnerabilidad que afecta al código JavaScript

C – Ninguna respuesta es correcta

D – Es una técnica para redireccionar al usuario hacia otro servidor

13 - ¿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 – HoneyNets

C – IDS

D – HoneyPots

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

A – Escritura

B – Ejecución

C – Borrado

D – Lectura

E – Todas las opciones

15 - ¿Cuál de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS?

A – Filtrado – Identificación – Acción

B – Recolección – Análisis – Respuesta

C – Ninguna de los anteriores

D – Recolección – Identificación – Clasificación

16 – A qué tipo de equipo se está refiriendo la siguiente definición?

“Divide la LAN en varios segmentos limitando el tráfico a uno o más segmentos en vez de permitir la difusión de paquetes por todos los puertos”

A – Switch

B – Router

C – Bridge

D – Hub

17 - ¿Cuál de los siguientes elementos no compone la lista de técnicas de OWASP Top-Ten Proactive Controls?

A – Implement Appropiate Access Controls

B – Validate All Inputs

C – Parameterize Queries

D – Use Virtual Keyboard in the Login

E – Encode Data

18 – Indique el tipo de ataque correspondiente a la siguiente definición: “[…] ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada.”

A – Falsificación de peticiones en sitios cruzados (CSRF)

B – Inyección

C – Referencia directa insegura a objetos

D – XSS-Cross Site Scripting

19 – 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 – Referencia directa insegura a objetos

B – Inyección

C – Falsificación de peticiones en sitios cruzados (CSRF)

D – Perdida de autenticación y gestión de sesiones

20 - ¿Cuál de los siguientes tipos no corresponde a la lista OWASP de 10 ataques más frecuentes?

A – Inyección

B – Control de accesos sin contraseñas seguras

C – Perdida de autenticación y gestión de sesiones

D – Falsificación de peticiones en sitios cruzados (CSRF)

21 - ¿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 – Referencia Directa Insegura a Objetos

B – Ausencia de Control de Acceso a Funciones

C – Falsificación de Peticiones en Sitios Cruzados (CSRF)

D – Secuencia de Comandos en Sitios Cruzados (XSS)

22 - ¿Cuál de las siguientes características no están asociadas a los firewalls?

A – Alta disponibilidad (AD)

B – Balanceo de carga (BCFW)

C – Filtrados de contenidos / Anti-spam

D – Almacenamiento de datos de negocio

23 - ¿Cuál de los siguientes elementos NO está catalogado como una Acción Hostil en Seguridad Física?

A – Sabotaje

B – Fraude

C – Inundación

D – Robo

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

A – Confidencialidad

B – Identificación

C – Disponibilidad

D – Ninguno

25 - ¿Cuál de los siguientes elementos NO se encuentra dentro de los Controles de Acceso Interno de la seguridad lógica?

A – Ninguno

B – Contraseñas

C – Etiquetas de seguridad

D – Listas de control de accesos

26 – Seleccione la opción según la definición de amenaza: “Entendemos por amenaza aquella situación de daño cuyo …”

A – Riesgo de producirse es significativo

B – Impacto genera una detención total del sistema

C – Origen se encuentra en el código de la aplicación

D – Impacto no afecta a la funcionalidad del sistema

27 - ¿Cuál de los siguientes puntos no es un atributo del protocolo TCP?

A – No es orientado a conexión

B – Un paquete tiene un numero de puerto origen y destino

C – Corre sobre IP

D – Cada paquete tiene un numero de secuencia y un flag

28 - ¿Cuál de los siguientes elementos se utiliza con el fin de capturar tramas de red?

A – Sniffer

B – Ninguno de los anteriores

C – IDS

D – Firewall Personal

29 - ¿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 – DMZ

C – Router

D – LBA

30 - ¿En qué zona ubica al ataque de Inyección?

A – Área de Servidor

B – Área de Red

C – Área de Cliente

D - Ninguna