1- ¿A que 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. Active X
   C. JavaScript
   D. Todas son correctas

3- ¿Cuál 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- ¿Cuál de estas afirmaciones es verdadera con relación a los Firewalls?
   A. No protege de ataques internos
   B. No protege de ataques internos
   C. No protege de todos los ataques dañinos
   D. Todas las anteriores

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 puerto 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. Es una vulnerabilidad que afecta al código JavaScript
   D. Ninguna respuesta es correcta

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- ¿Como 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 red 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 si se ha introducido cambios en el sistema de archivos

12- ¿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

13- ¿Cuál de los siguientes elementos corresponde a una Modalidad de Acceso a la información en Seguridad Lógica?
A. Escritura
B. Ejecución
C. Cifrado
D. Lectura
E. Todas las opciones

14- ¿Cuál de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS?
A. Filtrado – Identificación - Acción
B. Recolección - Análisis - Respuesta
C. Ninguno de los anteriores
D. Recolección – Identificación - Clasificación

15- 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 los paquetes por todos los puertos”
A. Switch
B. Router
C. Bridge
D. Hub

16- ¿Cuál de los siguientes elementos no compone la lista de técnicas de OWASP TopTen?
A. Implement Appropiate Access Controls
B. Validate All Inputs
C. Parameterize Queries
D. Use Virtual Keyboard in the Login

17- Indique el tipo de ataque correspondiente a la siguiente definición: "[...] ocurren cada vez que una aplicación tome 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

18- Indique el tipo de ataque correspondiente a la siguiente definición: “ocurre cuando datos no confiables son enviados a un interprete 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. Referencia directa insegura a objetos
B. Inyección
C. Falsificación de peticiones en sitios cruzados (CSRF)
D. Perdida de autenticación y gestión de sesiones

19- ¿Cuál de los siguientes tipo no corresponde a la lista OWASP de los 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)

20- ¿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

21- ¿Cuál de los siguientes elementos NO está catalogado como una Acción Hostil en Seguridad física?
A. Sabotaje
B. Fraude
C. Inundación
D. Robo

22- ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID ?
A. Confidencialidad
B. Identificación
C. Disponibilidad
D. Ninguno

23- ¿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 acceso

24- 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

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

A. Sniffers
B. Ninguno de los anteriores
C. IDS
D. Firewall Personal

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

A. Área de servidor
B. Área de red
C. Área de cliente
D. Ninguno

27- ¿Cuál de los siguientes elementos no forma parte del OWASP Top-Ten?

A. Referencia Directa Insegura A objetos
B. Redirecciones y reenvíos no válidos
C. Configuración de Seguridad Incorrecta
D. Denegación de Servicio

28- Indique a que termino se asocia la siguiente definición: "[...] es la propiedad que busca mantener los datos libres de modificaciones no autorizadas."

A. Integridad
B. Disponibilidad
C. Consistencia
D. Confidencialidad

29- ¿En qué zona ubica al ataque de Exposición de datos sensibles?

A. Área de Cliente
B. Área de Red
C. Área de Servidor
D. Área de Red y Área de Servidor

30- ¿A qué se denomina "Learning Mode" en el contexto de la implementación de un WAF?

A. Al modo de operación donde la herramienta registra la actividad normal de la aplicación para que posteriormente pueda ser utilizada a fin de generar reglas.
B. Al modo de operación donde se permite que el usuario acceda a la aplicación para generar los ataques que posteriormente serán bloqueados
C. A la capacitación del personal que llevara adelante la configuración de la herramienta
D. Ninguna de las anteriores

31- SYN Flood corresponde a una técnica utilizada para realizar un ataque de:

A. Inyección
B. Denegación de servicio
C. Control remoto de un servidor
D. Secuencia de Comandos en sitios cruzados (XSS)

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

A. SQL
B. Ninguno
C. LDAP
D. X-Path

34- ¿Que protocolo soporta la implementación de VPNs?

A. Ninguna de las opciones
B. IPSEC
C. Secure TCP
D. ICMP

35- ¿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

36- 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

37- 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 – Plan director

38- ¿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

39- Según la definición de “DAÑO” seleccione la respuesta correcta:

A. Debe ser cuantificable
B. Todas las respuestas
C. Ocurre solo cuando se inhabilita el sistema de forma completa
D. Se debe expresar en probabilidad de ocurrencia