1) ¿A que ataque del OWASP Top Ten se refiere la siguiente definicion: "El atacante puede ejecutar secuencias de comandos en el navegador de la victima.."?
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) ¿Cuál de los siguientes puntos NO corresponde a un tipo de vulnerabilidad? A) Debidas al uso
B) Debidas al diseño
C) Debidas a la implementacion
D) Ninguna de las anteriores

4) ¿Cuál de estas afirmaciones es verdadera en relacion a los Firewalls?
A) No protege de accesos no autorizados
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 tecnica para redireccionar al usuario hacia otro servidor.
B) Es un ataque de alteracion de datos no autorizados
C) Ninguna respuesta es correcta
D) Es una vulnerabilidad que afecta al codigo javascript

7) ¿Cuál de los siguientes factores no es evaluado por la OWASP para determinar los riesgos inclui dos en el proyecto Top Ten?
A) Vectores de Ataque
B) Detectabilidad de debilidades
C) Impacto tecnico
D) Impacto en el negocio

8) ¿Qué es un bugtraq?
A) Ninguna de las opciones es correcta
B) Es una lista de notificaciones 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 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 autenticacion 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 via email sobre cambios en el sistema de archivos.
C) Identificar los cambios realizados en los archivos del sistema
D) Identificar al usuario que ha producido cambios en el sistema de archivos.

12) ¿A qué tipo de equipo se esta refiriendo la siguiente definición? "Analiza el trafico de la red para tratar de detectar patrones sospechosos que indiquen ataques o intenciones de ataques contra algun recurso. Una vez identificados, puede tomar ciertas medidas contra ese tipo de trafico, como generar alertas o inclusive bloquear o descartar el tráfico que viene de ese origen.
A) Statefulls
B) HoneyNets
C) IDS
D) HonetPots

13) ¿Cuál de los siguientes elementos corresponde a una modalidad de acceso a la informacion en seguridad logica?
A) Escritura
B) Ejecución
C) Borrado
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 esta refiriendo la siguiente definicion? "Divide la LAN en varios segmen tos limitando el trafico a uno o mas 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 tecnicas de OWASP Top Ten Proctive Controls?

A) Implement Appropiate Access Controls
B) Validate All Inputs
C) Parameterize Queries
D) Use Virtual Keyboard in the login
E) Encode data

17) Indique el tipo de ataque correspondiente a la siguiente definicion: "[…] ocurren cada vez que una aplicación toma datos no confiables y los envia 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 definicion: "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) Pérdida de autenticación y gestion de sesiones

19) ¿Cuál de los siguientes tipos no corresponde a la lista OWASP de los ataques mas frecuentes? A) Inyección
B) Control de accesos sin contraseñas seguras
C) Pérdida de autenticación y gestión de sesiones
D) Falsificación de peticiones en sitios cruzados (CSRF)

20) ¿A qué ataque del OWASP Top Ten se refiere la siguiente definición: "El atacante puede ejecutar secuencias de comandos en el navegador de la victima…"?
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)

21) ¿Cuál de las siguientes características no estan 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

22) ¿Cuál de los siguientes elementos NO esta catalogado como una Accion Hostil en Seguridad Física?
A) Sabotaje
B) Fraude
C) Inundacion
D) Robo

23) ¿Cuál de los siguiente elementos NO forma parte de la pirámide ID?
A) Confidencialidad
B) Identificación

C) Disponibilidad
D) Ninguno

24) ¿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

25) 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

26) ¿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 de origen y destino
C) Corre sobre IP
D) Cada paquete tiene un numero de secuencia y un flag

27) ¿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

28) ¿En qué zona ubica al ataque de inyección?
A) Area de servidor
B) Area de Red
C) Area de Cliente
D) Ninguna

29) ¿Cuál de los siguientes elementos no forma parte del OWASP Top-Ten?
A) Referencia directa insegura a objetos
B) Redirecciones y reenvios no validos
C) Configuracion de seguridad incorrecta.
D) Denegación de servicio

30) 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

31) ¿En qué zona ubica al ataque de exposicion de datos sensibles?
A) Area del cliente

B) Area de Red
C) Area de Servidor
D) Area de red y area de servidor

32) ¿A que 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 seran bloqueados.
C) A la capacitacion del personal que llevara adelante la configuración de la herramienta.
D) Ninguna de las opciones.

33) SYN Flood corresponde a una tecnica utilizada para realizar un ataque de…

A) Inyeccion
B) Denegación de servicio
C) Control remoto de un servidor
D) Secuencia de comandos en sitios cruzados(XSS)

34) ¿Cuál de las siguientes tecnologías no puede ser utilizada en un ataque de inyeccion?
A) SQL
B) LDAP
C) X-Path
D) Ninguna

35) ¿Cuál de estas afirmaciones es verdadera en relacion a los firewalls?
A) No protege de accesos no autorizados
B) No protege de todos los ataques dañinos
C) No protege de ataques internos
D) Todas las anteriores

36) ¿Qué protocolo soporta la implementacion de VPNs?
A) IPSec
B) Secure TCP
C) ICMP
D) Ninguna de las opciones.

37) Seleccione el tipo de ataque correspondiente a la siguiente definicion: " es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legitimos."
A) Inyeccion
B) Perdida de autenticacion
C) Tampering
D) Denegación de servicio

38) ¿Cuál de estos elementos corresponde a la siguiente definicion: "Se trata de un dispositivo que analiza el tráfico 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

39) Explique el ataque por injection comparandolo y asociandolo con el de XSS. Adicionalmente indique que medidas se recomiendan para proteger a una aplicación de este ataque?

RTA:**Ataque por inyección (Injection Attack):**
Es un tipo de vulnerabilidad que ocurre cuando datos no confiables (generalmente introducidos por el usuario) son enviados a un intérprete como parte de un comando o consulta. El ejemplo más común es la **inyección SQL**, donde un atacante puede manipular una consulta SQL para acceder, modificar o eliminar información de una base de datos.

Cross-Site Scripting (XSS):
Es un tipo de ataque que se produce cuando una aplicación web permite la inserción de scripts maliciosos (normalmente en JavaScript) en el contenido que se muestra a otros usuarios. A diferencia de la inyección SQL, XSS afecta principalmente al **navegador del usuario**, permitiendo robar cookies, secuestrar sesiones o mostrar contenido fraudulento.

Comparación y asociación:

- Ambos ataques aprovechan la **falta de validación y saneamiento** de datos de entrada.
- La **inyección SQL** apunta al **servidor** (base de datos), mientras que **XSS** apunta al **cliente** (navegador).
- Los dos pueden usarse para **robar información confidencial** o alterar el comportamiento esperado de la aplicación.

Medidas de protección comunes:

- Validar y sanear siempre todas las entradas del usuario.
- Usar consultas preparadas (prepared statements) con parámetros en lugar de concatenar datos en consultas SQL.
- Escapar caracteres especiales en los datos enviados a la base de datos o al navegador.
- Implementar filtros de contenido para prevenir scripts maliciosos en campos que se muestran a otros usuarios.

40) Desarrolle la definicion y funcion de un IDS explique sus diferencias con un IPS y un Firewall

RTA:**IDS (Intrusion Detection System – Sistema de Detección de Intrusos):**
Es una herramienta o sistema que **monitorea** el tráfico de red o actividades en un sistema informático con el objetivo de **detectar comportamientos sospechosos** o violaciones de políticas de seguridad. No bloquea automáticamente, sino que **genera alertas** para que el administrador tome medidas.

Función del IDS:

- Detectar intentos de intrusión o patrones de ataque conocidos.
- Registrar eventos de seguridad.
- Generar alertas en tiempo real.
- A veces puede integrarse con otras herramientas para automatizar respuestas

  Resumen:

  IDS detecta y alerta, pero no interviene directamente.

  IPS es como un IDS más avanzado que puede **detener** el ataque en tiempo real.

  Firewall controla qué tráfico entra o sale, basándose en reglas predefinidas de puertos, direcciones IP o protocolos.