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 victima…”?

1. **Secuencia de Comandos en Sitios Cruzados (XXS)**
2. Ausencia de Control de Acceso a Funciones
3. Falsificación de Peticiones en Sitios Cruzados (CSRF)
4. Referencia Directa Insegura a Objetos.

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

1. Java Applet
2. Activex
3. JavaScript
4. **Todas las anteriores**

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

1. Debidas al uso
2. Debidas al diseño
3. Debidas a la implementación
4. **Ninguna de las anteriores**

4- Cual de estas afirmaciones es verdadera en relación con los firewalls?

1. No protege de accesos no autorizados
2. No protege de ataques internos
3. **Todas las anteriores**
4. No protege de todos los ataques dañinos

5- Cual de los siguientes puntos no es atributo del protocolo TCP? **(no lo dice la PPT)**

1. **No es orientado a conexión**
2. Corre sobre IP
3. Cada paquete tiene un numero de secuencia y un flag
4. Un paquete tiene un numero de puerto origen y destino.

6- Que se entiende por tampering?

1. Es una técnica para redireccionar al usuario hacia otro servidor
2. **Es un ataque de alteración de datos no autorizados**
3. Ninguna respuesta es correcta.
4. Es una vulnerabilidad que afecta al código JavaScript

7- Cual de los siguientes factores NO es evaluado por la OWASP para determinar los riesgos incluidos en el proyecto Top-Ten? **(No figura ninguna de las 4 en la PPT)**

1. Vectores de ataque
2. Detectabilidad de debilidades
3. Impacto técnico
4. Impacto en el negocio

8- Que es un bugtraq?

1. **Es una lista de notificación sobre vulnerabilidades encontradas en software y hardware**
2. Es una variante de virus o troyano
3. Es un software diseñado para buscar vulnerabilidades
4. Ninguna de las opciones es correcta

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.)?

1. **DMZ**
2. B2B
3. Router
4. LBA

10- Que es un firewall?

1. **Un dispositivo que permite bloquear o filtrar el acceso entre dos redes; usualmente una privada y otra externa.**
2. Un dispositivo de antivirus de red
3. Una librería de software que permite asegurar una aplicación web
4. Un dispositivo que permite la autenticación en aplicaciones

11- Cual es la principal función de un comprobador de integridad?

1. **Identificar archivos que han sido alterados en el sistema de archivos.**
2. Notificar vía email sobre cambios en el sistema de archivos
3. Identificar los cambios realizados en los archivos del sistema
4. Identificar al usuario introducido cambios en el sistema de archivos.

12- A que tipo de equipo se está refiriendo la siguiente definición: “Analiza el trafico 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 trafico que viene de ese origen”.

1. Statefulls
2. HoneyNets
3. **IDS**
4. HoneyPots

13- Cual de los siguientes elementos corresponde a una modalidad de acceso a la información en Seguridad Lógica?

1. Escritura
2. Ejecución
3. Borrado
4. Lectura
5. **Todas las opciones**

14- Cual de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS?

1. Filtrado – Identificación – Acción
2. **Recolección – Análisis – Respuesta**
3. Ninguno de los anteriores
4. Recolección – Identificación – Clasificación

15- A que tipo de equipo se esta refiriendo a la siguiente definición: "Divide la LAN en varios segmentos limitando el tráfico a uno o mas segmentos en vez de permitir la difusión de los paquetes por todos los puertos". **(no lo dice en la PPT)**

1. **Switch**
2. Router
3. Bridge
4. Hub

16- Cual de los siguientes elementos no compone la lista de técnicas de OWASP Top Ten Proactive Controls? **(no lo dice la PPT)**

1. Implement Appropiate Access Controls
2. Validate All Inputs
3. Parameterize Queries
4. **Use Virtual Keyboard in the Login**
5. Encode Data

17- Indique el tipo de ataque correspondiente a la siguiente definición: " … ocurre cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada".

1. Falsificación de peticiones en sitios cruzados (CSRF)
2. Inyección
3. Referencia directa insegura a objetos
4. **XSS Cross Site Scripting**

18- Indique tipo de ataque a la siguiente definición: "… ocurren 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 intencionales o acceder a datos no autorizados".

1. Referencia directa insegura a objetos,
2. **Inyección**
3. falsificación de peticiones en sitios cruzados (CSRF)
4. Perdida de autenticación y gestión de sesiones

19- Cual de los siguientes tipos no corresponde a la lista DASP de 10 ataques más frecuentes?

1. Inyección
2. **Control de accesos sin contraseñas seguras**
3. Perdida de autenticación y gestión de sesiones
4. Falsificación de peticiones en sitios cruzados (CSRF)

20- Cual de las siguientes características NO están asociadas a los firewalls?

1. Alta disponibilidad (ad)
2. Balanceo de carga (BCFW)
3. Filtrados de contenidos/ anti-spams
4. **Almacenamiento de datos de negocio**

21- Cual de los siguientes elementos NO esta catalogado como una Acción Hostil en Seguridad Física?

1. Sabotaje
2. Fraude
3. **Inundación**
4. Robo

22- Cual de los siguientes elementos NO forma parte de la pirámide ID?

1. Confidencialidad
2. **Identificación**
3. Disponibilidad
4. Ninguno

23- Cual de los siguientes elementos NO se encuentra dentro de los controles de Acceso Interno de la Seguridad Lógica?

1. Contraseñas
2. Etiquetas de Seguridad
3. Listas de Control de Accesos
4. **Ninguno**

24- Seleccione la opción según la definición de amenaza: “Entendemos por amenaza, aquella situación de daño cuyo… “

1. **Riesgo de producirse es significativo**
2. Impacto genera una detención total del sistema
3. Origen se encuentra en el código de la aplicación
4. Impacto no afecta a la funcionalidad del sistema

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

1. **Sniffer**
2. IDS
3. Ninguno de los anteriores
4. Firewall Personal

26- En que zona ubica el ataque de Inyección?

1. **Área de Servidor**
2. Área de Red
3. Área de Cliente
4. Ninguna

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

1. Referencia Directa Insegura a Objetos
2. Redirecciones y reenvíos no validos
3. Configuración de Seguridad Incorrecta
4. **Denegación de Servicio**

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

1. **Integridad**
2. Disponibilidad
3. Consistencia
4. Confidencialidad

29- En que zona ubica el ataque de Exposición de datos sensibles? **(no lo dice la PPT)**

1. **Área de Cliente**
2. Área de Red
3. Área de Servidor
4. Área de Red y Área de Servidor

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

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

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

1. Inyección
2. **Denegación de Servicio**
3. Control remoto de un servidor
4. Secuencia de Comandos en Sitios Cruzados (XSS)

32- Cuales de las siguientes tecnologías NO puede ser utilizada en un ataque de Inyección?

1. SQL
2. LDAP
3. X-Path
4. **Ninguna**

33- Que protocolo soporta la implementación de VPNs?

1. **IPSec**
2. Secure TCP
3. ICMP
4. Ninguna de las opciones