1er Parcial - Seguridad (2016)

1. ¿ Cuál de los siguientes elementos no forma parte del OWASP Top-Ten?
   A. Referencia Directa Insegura A objetos
   B. Redirecciones y reenvíos no validos
   C. Configuración de seguridad Incorrecta
   D. Denegación de Servicio

2. 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

3. ¿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 - Un dispositivo que permite la autenticación de aplicaciones.
   D - Una librería de software que permite asegurar una aplicación web.

4. ¿En qué zona ubica al ataque de exposición de Datos Sensibles?
   A - Área de Cliente
   B - Área de Red
   B - Área de Servidor
   D - Área de Red y Área de Servidor

5. ¿Cuál de estas tecnologías es considerada generadora de riesgo por ser ejecutada en el lado del cliente?
   A - Java Applet
   B - ActiveX
   C - Javascript
   D - Todas las anteriores

6. ¿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 ataque que posteriormente serán bloqueados.
   C – A la capacitación del personal que llevara adelante la configuración de la herramienta
   D – Ninguna de las anteriores

7. 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 de Sitios Cruzados (XSS)

8. ¿Cuál de las siguientes tecnologías no puede ser utilizada en un ataque de inyección?
   A. SQL
   B. Ninguna
   C. LDAP
   D. X-Patch

9. ¿Cuál de estas afirmaciones es verdadera en relación a los Firewalls?
   A. Todas las anteriores
   B. No protege de accesos no autorizados
   C. No protege de todos los ataques dañinos
   D. No protege de ataques internos

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

11. ¿Qué es un bugtraq?
    A. Es una lista de notificación sobre vulnerabilidades encontradas en un software y hardware
    B. Es un software diseñado para buscar vulnerabilidades
    C. Es una variante de virus o troyano
    D. Ninguna de las opciones es correcta

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 que 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 ataque contra algún recurso. Una vez identificados, puede tomar ciertas medidas contra ese tipo de trafico, como generar alertas o inclusive bloquear o descartar el trafico que viene de ese origen.”

    A. Statefull
    B. HoneyNets
    C. IDS
    D. HonetPosts

14. ¿Cuál de los siguientes elementos corresponde a una Modalidad de Acceso a la información de 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. Ninguno de los anteriores
    D. Recolección – Identificación – Clasificación

16. ¿A qué tipo de equipo se esta refiriendo la siguiente definición? “Divide la LAN en varios segmentos limitando al trafico a uno o mas segmentos en vez de permitir la difusión de los paquetes por todos los puestos”
    A. Switch
    B. Router
    C. Bridge
    D. Hub

17. ¿Cuál de los siguientes elementos no compone la lista de técnicas de OWASP TopTen 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 al 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 Scriping

19. 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.

20. ¿Cuál de los siguientes tipos NO corresponde a la lista OWASP de 10 ataques más frecuentes?
    A. Inyección
    B. Control de accesos sin contraseña seguras
    C. Perdida de autentificación y gestión de sesión
    D. Falsificación de peticiones en sitios cruzados (CSRF)

21. ¿A que ataque del OWASP Top-Ten se refiere la siguiente definición : “El ataque 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 contenido / Anti-Spam
    D. Almacenamiento de datos de negocio

23. ¿Cuál de los siguientes elementos NO esta 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. Lista de control de acceso

26. Seleccione la opción según la definición de amenaza: “Entendemos como 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 que zona ubica al ataque de Inyección?
    A. Area de servidor
    B. Area de Red
    C. Area de Cliente
    D. Ninguna