# 1er Parcial - Seguridad (2016)

1. ¿ Cuál de los siguientes elementos no forma parte del OWASP Top-Ten?
2. Referencia Directa Insegura A objetos
3. Redirecciones y reenvíos no validos
4. Configuración de seguridad Incorrecta
5. Denegación de Servicio
6. 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

1. ¿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.

1. ¿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

1. ¿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

1. ¿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

1. SYN Flood corresponde a una técnica utilizada para realizar un ataque de …
2. Inyección
3. Denegación de servicio
4. Control remoto de un servidor
5. Secuencia de Comandos de Sitios Cruzados (XSS)
6. ¿Cuál de las siguientes tecnologías no puede ser utilizada en un ataque de inyección?
7. SQL
8. Ninguna
9. LDAP
10. X-Patch
11. ¿Cuál de estas afirmaciones es verdadera en relación a los Firewalls?
12. Todas las anteriores
13. No protege de accesos no autorizados
14. No protege de todos los ataques dañinos
15. No protege de ataques internos
16. ¿Qué protocolo soporta la implementación de VPNs?
17. Ninguna de las opciones
18. IPSec
19. Secure TCP
20. ICMP
21. ¿Qué es un bugtraq?
22. Es una lista de notificación sobre vulnerabilidades encontradas en un software y hardware
23. Es un software diseñado para buscar vulnerabilidades
24. Es una variante de virus o troyano
25. Ninguna de las opciones es correcta
26. ¿Qué se entiende por “tampering”?
27. Es un ataque de alteración de datos no autorizados
28. Es una vulnerabilidad que afecta al código javascript
29. Ninguna respuesta es correcta
30. Es una técnica para redireccionar al usuario hacia otro servidor
31. ¿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.”
32. Statefull
33. HoneyNets
34. IDS
35. HonetPosts
36. ¿Cuál de los siguientes elementos corresponde a una Modalidad de Acceso a la información de Seguridad Lógica?
37. Escritura
38. Ejecución
39. Borrado
40. Lectura
41. Todas las opciones
42. ¿Cuál de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS?
43. Filtrado – Identificación – Acción
44. Recolección – Análisis – Respuesta
45. Ninguno de los anteriores
46. Recolección – Identificación – Clasificación
47. ¿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”
48. Switch
49. Router
50. Bridge
51. Hub
52. ¿Cuál de los siguientes elementos no compone la lista de técnicas de OWASP TopTen Proactive Controls?
53. Implement Appropiate Access Controls
54. Validate All Inputs
55. Parameterize Queries
56. Use Virtual Keyboard in the Login
57. Encode Data
58. 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”
59. Falsificación de peticiones en sitios cruzados (CSRF)
60. Inyección
61. Referencia directa insegura a objetos
62. XSS – Cross Site Scriping
63. 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.”
64. Referencia directa insegura a objetos
65. Inyección
66. Falsificación de peticiones en sitios cruzados (CSRF)
67. Perdida de autenticación y gestión de sesiones.
68. ¿Cuál de los siguientes tipos NO corresponde a la lista OWASP de 10 ataques más frecuentes?
69. Inyección
70. Control de accesos sin contraseña seguras
71. Perdida de autentificación y gestión de sesión
72. Falsificación de peticiones en sitios cruzados (CSRF)
73. ¿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.”?
74. Referencia Directa Insegura a Objetos
75. Ausencia de Control de Acceso a Funciones
76. Falsificación de Peticiones en Sitios Cruzados (CSRF)
77. Secuencia de Comandos en Sitios Cruzados (XSS)
78. ¿Cuál de las siguientes características no están asociadas a los Firewalls?
79. Alta disponibilidad (AD)
80. Balanceo de carga (BCFW)
81. Filtrados de contenido / Anti-Spam
82. Almacenamiento de datos de negocio
83. ¿Cuál de los siguientes elementos NO esta catalogado como una Acción Hostil en Seguridad Física?
84. Sabotaje
85. Fraude
86. Inundación
87. Robo
88. ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID?
89. Confidencialidad
90. Identificación
91. Disponibilidad
92. Ninguno
93. ¿Cuál de los siguientes elementos NO se encuentra dentro de los Controles de Acceso Interno de la seguridad lógica?
94. Ninguno
95. Contraseñas
96. Etiquetas de seguridad
97. Lista de control de acceso
98. Seleccione la opción según la definición de amenaza: “Entendemos como amenaza aquella situación de daño cuyo…”
99. Riesgo de producirse es significativo
100. Impacto genera una detención total del sistema
101. Origen se encuentra en el código de la aplicación
102. Impacto no afecta a la funcionalidad del sistema
103. ¿Cuál de los siguientes puntos NO es un atributo del protocolo TCP?
104. No es orientado a conexión
105. Un paquete tiene un numero de puerto origen y destino
106. Corre sobre IP
107. Cada paquete tiene un numero de secuencia y un flag
108. ¿Cuál de los siguientes elementos se utiliza con el fin de capturar tramas de red?
109. Sniffer
110. Ninguno de los anteriores
111. IDS
112. Firewall Personal
113. ¿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.)?
114. B2B
115. DMZ
116. Router
117. LBA
118. ¿En que zona ubica al ataque de Inyección?
119. Area de servidor
120. Area de Red
121. Area de Cliente
122. Ninguna