**PREGUNTAS PARCIAL 1 – SCAW**

**Unidad 1**

1. ¿Cuál 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
2. 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. )?
3. **DMZ**
4. B2B
5. Router
6. LBA
7. ¿Qué es un firewall?
8. **Un dispositivo que permite bloquear o filtrar el acceso entre dos redes; usualmente una privada y otra externa.**
9. Un dispositivo de antivirus de red
10. Una librería de software que permite asegurar una aplicación web
11. Un dispositivo que permite la autenticación en aplicaciones
12. ¿Cuál es la principal función de un comprobador de integridad?
13. **Identificar archivos que han sido alterados en el sistema de archivos.**
14. Notificar vía email sobre cambios en el sistema de archivos
15. Identificar los cambios realizados en los archivos del sistema
16. Identificar al usuario introducido cambios en el sistema de archivos.
17. 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”.
18. Statefulls
19. HoneyNets
20. **IDS**
21. HoneyPots
22. ¿Cuál de los siguientes elementos corresponde a una modalidad de acceso a la información en Seguridad Lógica?
23. Escritura
24. Ejecución
25. Borrado
26. Lectura
27. **Todas las opciones**
28. ¿Cuál de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS?
29. Filtrado – Identificación – Acción
30. **Recolección – Análisis – Respuesta**
31. Ninguno de los anteriores
32. Recolección – Identificación – Clasificación
33. ¿Cuál de las siguientes características NO están asociadas a los firewalls?
34. Alta disponibilidad (ad)
35. Balanceo de carga (BCFW)
36. Filtrados de contenidos/ anti-spam
37. **Almacenamiento de datos de negocio**
38. ¿Cuál de los siguientes elementos NO está catalogado como una Acción Hostil en Seguridad Física?
39. Sabotaje
40. Fraude
41. **Inundación**
42. Robo
43. ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID?
44. Confidencialidad
45. **Identificación**
46. Disponibilidad
47. Ninguno
48. ¿Cuál de los siguientes elementos NO se encuentra dentro de los controles de Acceso Interno de la Seguridad Lógica?
49. Contraseñas
50. Etiquetas de Seguridad
51. Listas de Control de Accesos
52. **Ninguno**
53. Seleccione la opción según la definición de amenaza: “Entendemos por amenaza, aquella situación de daño cuyo… “
54. **Riesgo de producirse es significativo**
55. Impacto genera una detención total del sistema
56. Origen se encuentra en el código de la aplicación
57. Impacto no afecta a la funcionalidad del sistema
58. Indique a que termino asocia la siguiente definición: “… es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.”
59. **Integridad**
60. Disponibilidad
61. Consistencia
62. Confidencialidad
63. ¿A qué se denomina “Learning Mode” en el contexto de la implementación de un WAF?
64. **Al modo de operación donde la herramienta registra la actividad normal de la aplicación para posteriormente pueda ser utilizada a fin de generar reglas.**
65. Al modo de operación donde se permite que el usuario acceda a la aplicación para generar los ataques que posteriormente serán bloqueados
66. A la capacitación del personal que llevara adelante la configuración de la herramienta
67. Ninguna de las opciones
68. ¿Qué protocolo soporta la implementación de VPNs?
69. **IPSec**
70. Secure TCP
71. ICMP
72. Ninguna de las opciones
73. ¿Cuáles de las siguientes son ítems participes de la Seguridad Lógica?
74. Control de Acceso
75. Roles
76. Transacciones
77. **Todas las otras opciones**
78. ¿Cuáles de los siguientes ítems no son evaluados en la seguridad física?
79. Tipos de desastres
80. **Limitaciones a los servicios**
81. Acciones hostiles
82. Ninguna de las otras opciones
83. El hash:
84. Función o método matemático reversible para generar un valor que represente de manera casi univoca un dato.
85. **Función o método matemático no reversible para generar un valor que represente de manera casi univoca un dato**
86. Función o método matemático no reversible para generar un valor que represente de manera univoca un dato
87. Ninguna de las otras opciones

RECUPERATORIO

1. ¿Cuál de estas características no corresponde al Control de Acceso Interno?:
   1. Contraseñas
   2. Cifrado
   3. Etiquetas de Seguridad
   4. **Ninguna de las anteriores**
2. ¿Qué es el hash?
   1. Función reversible con entrada de tamaño variable y salida de tamaño variable.
   2. **Función no reversible con entrada de tamaño variable y salida de tamaño fijo.**
   3. Función no reversible con entrada de tamaño variable y salida de tamaño variable.
   4. Función reversible con entrada de tamaño variable y salida de tamaño fijo.
3. Según la definición de Daño:
   1. Se produce cuando el sistema/aplicación deja de funcionar en su totalidad.
   2. Es significativo.
   3. **Es cuantificable**
   4. Ninguna de las anteriores.
4. ¿Cuál no es un factor de seguridad biométrico?
   1. Temperatura corporal
   2. Huella digital
   3. Control de voz
   4. **Ninguna de las anteriores**
5. Según el Application DoS:
   1. **Se produce cuando un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios debido al consumo del ancho de banda o sobrecarga de recursos computacionales**
   2. Se inunda con paquetes o conexiones de red sobrecargando el equipamiento de la red de servidores o ancho de banda.
   3. Genera solicitudes maliciosas a un servicio, saturándolo o haciéndolo entrar en modo de espera.
   4. Todas las anteriores

**Unidad 2**

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…”?
2. **Secuencia de Comandos en Sitios Cruzados (XSS)**
3. Ausencia de Control de Acceso a Funciones
4. Falsificación de Peticiones en Sitios Cruzados (CSRF)
5. Referencia Directa Insegura a Objetos.
6. ¿Cuál de estas tecnologías es considerada generadora de riesgo por ser ejecutada en el cliente?
7. Java Applet
8. Activex
9. JavaScript
10. **Todas las anteriores**
11. ¿Cuál de los siguientes puntos NO corresponde a un tipo de vulnerabilidad?
12. Debidas al uso
13. Debidas al diseño
14. Debidas a la implementación
15. **Ninguna de las anteriores**
16. ¿Qué se entiende por tampering?
17. Es una técnica para redireccionar al usuario hacia otro servidor
18. **Es un ataque de alteración de datos no autorizados**
19. Ninguna respuesta es correcta.
20. Es una vulnerabilidad que afecta al código JavaScript
21. ¿Cuál 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)**
22. Vectores de ataque
23. Detectabilidad de debilidades
24. Impacto técnico
25. Impacto en el negocio
26. ¿Qué es un bugtraq?
27. **Es una lista de notificación sobre vulnerabilidades encontradas en software y hardware**
28. Es una variante de virus o troyano
29. Es un software diseñado para buscar vulnerabilidades
30. Ninguna de las opciones es correcta
31. 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”.
32. Falsificación de peticiones en sitios cruzados (CSRF)
33. Inyección
34. Referencia directa insegura a objetos
35. **XSS Cross Site Scripting**
36. Indique tipo de ataque a la siguiente definición: “… ocurren cuando datos no confiables son enviados a un intérprete 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”.
37. Referencia directa insegura a objetos,
38. **Inyección**
39. falsificación de peticiones en sitios cruzados (CSRF)
40. Perdida de autenticación y gestión de sesiones
41. ¿Cuál de los siguientes tipos no corresponde a la lista DASP de 10 ataques más frecuentes?
42. Inyección
43. **Control de accesos sin contraseñas seguras**
44. Perdida de autenticación y gestión de sesiones
45. Falsificación de peticiones en sitios cruzados (CSRF)
46. ¿Cuál de los siguientes elementos se utiliza con el fin de capturar tramas de red?
47. **Sniffer**
48. IDS
49. Ninguno de los anteriores
50. Firewall Personal
51. ¿En qué zona ubica el ataque de Inyección?
52. **Área de Servidor**
53. Área de Red
54. Área de Cliente
55. Ninguna
56. ¿Cuál de los siguientes elementos no forma parte del OWASP Top-Ten?
57. Referencia Directa Insegura a Objetos
58. Redirecciones y reenvíos no validos
59. Configuración de Seguridad Incorrecta
60. **Denegación de Servicio**
61. SYN Flood corresponde a una técnica utilizada para realizar ataque de…
62. Inyección
63. **Denegación de Servicio**
64. Control remoto de un servidor
65. Secuencia de Comandos en Sitios Cruzados (XSS)
66. ¿Cuáles de las siguientes tecnologías NO puede ser utilizada en un ataque de Inyección?
67. SQL
68. LDAP
69. X-Path
70. **Ninguna**
71. ¿Cuál es el área de mayor control en un entorno web?
72. Área de cliente
73. Área de red
74. **Área de servidor**
75. Todas tienen el mismo nivel
76. Indique cual de estos ataques no corresponde a DoS
77. Slowloris
78. SMURF
79. **CSRF**
80. Syn Flood
81. ¿Cuál de los siguientes elementos no es calificado durante el proceso de evaluación de riesgos del top10?
82. **Agente de amenaza**
83. Impacto técnico
84. Explotabilidad
85. Detección de vulnerabilidad
86. Una aplicación que utiliza SOAP en una versión previa a la 1.2 y permite que las entidades sean pasadas a la infraestructura SOAP, es potencialmente vulnerable a:
87. XSS
88. **XXE**
89. Inyección
90. Pérdida de Control de Acceso
91. ¿Qué riesgos del Top10 2017 ha resuelto de la unión de dos riesgos de la versión anterior? Nota Referencia directa insegura a objetos y ausencia de control de acceso a funciones
92. **Pérdida de Control de Acceso**
93. Uso de componentes con vulnerabilidades conocidas
94. Inyección
95. Exposición de datos sensibles
96. ¿Cuál de los siguientes elementos NO es un control proactivo?
97. Validar todas las entradas
98. Implementas identidad digital
99. Proteger los datos en todas partes
100. **Ejecutar scanners de vulnerabilidades**
101. El uso de PBKDF2 esta asociado a que riesgo del Top10?
102. XXS-Cross Site Scripting
103. **Exposición de datos sensibles (A02 Fallas criptográficas)**
104. Registro y Monitoreo Insuficientes
105. Entidad Externa de XML

**Cosas a tener en cuenta tomadas en Recuperatorio**

Si en la consulta sobre inyección:

* Si pone código que tiene HTTP, la respuesta es CSRF.
* Si pone “inner…” refiere al DOM y es una característica del XSS – Basados en Dom
* Prevención de Inyección: La opción que no está en las prevenciones del resumen

**Preguntas que no están en las unidades**

1. ¿Cuál de los siguientes puntos no es atributo del protocolo TCP?
   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 de origen y destino
2. ¿Cuál de los siguientes factores NO es evaluado por la OWASP para determinar los riesgos incluidos en el proyecto Top-Ten?
   1. Vectores de ataque
   2. Detectabilidad de debilidades
   3. Impacto técnico
   4. Impacto en el negocio
3. ¿A qué tipo de equipo se está refiriendo a 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”?
4. **Switch**
5. Router
6. Bridge
7. Hub
8. ¿Cuál de los siguientes elementos no compone la lista de técnicas de OWASP Top Ten Proactive Controls?
9. Implement Appropiate Access Controls
10. Validate All Inputs
11. Parameterize Queries
12. **Use Virtual Keyboard in the Login**
13. Encode Data
14. ¿En qué zona ubica el ataque de Exposición de datos sensibles?
15. **Área de Cliente**
16. Área de Red
17. Área de Servidor
18. Área de Red y Área de Servidor