Comenzado el	lunes, 10 de junio de 2019, 14:04
Estado	Finalizado
Finalizado en	lunes, 10 de junio de 2019, 14:34
Tiempo empleado	29 minutos 23 segundos
Calificación	**47,00** de 60,00 (**78**%)

Pregunta **1**

Finalizado

Puntúa 6,00 sobre 8,00

[OWASP] Mediante el TOP A6 de OWASP (Security Misconfiguration) se busca : (Marque las respuestas correctas)

Seleccione una o más de una:

- a. Eliminar servicios y componentes innecesarios.
- b. Eliminar archivos / scripts de ejemplo y documentación.
- c. Eliminar usuarios preconfigurados o innecesarios.
- d. Gestionar la instalación de parches de sistema operativo.
- e. Cambiar el sistema de logging y reporte de errores.

Pregunta **2**

Finalizado

Puntúa 3,00 sobre 3,00

Seleccione la definición correcta de vulnerabilidad

Seleccione una:

- a. Implica la detección, análisis y control del Riesgo generado por una situación de vulnerabilidad técnica o no técnica.
- b. Es la aplicación de Parches.
- c. Es el escaneo de puertos y servicios.
- d. Es el Ethical Hacking o Pentesting.
- e. Es la revisiones o Auditorias de Seguridad.

Pregunta **3**

Finalizado

Puntúa 8,00 sobre 8,00

Recomendaciones para la gestión de vulnerabilidades (marque las respuestas correctas)

Seleccione una o más de una:

- [x] a. Realizar escaneos periódicos y sistemáticos a todos los activos identificados.
- [x] b. Desarrollar y mantener la Política de Seguridad y el Marco Normativo de la organización.
- [ ] c. Desclasificar la Información.
- [x] d. Identificar los riesgos asociados a cada uno de los activos en función de las vulnerabilidades detectadas.
- [x] e. Relevar y categorizar los Activos de Información en función del nivel de criticidad para el negocio.

Pregunta **4**

Finalizado

Puntúa 4,00 sobre 4,00

¿Cuándo un atacante obtiene datos, mediante algún tipo de engaño a un usuario desprevenido que tipo de ataque está utilizando?

Seleccione una:

- ( ) a. Ingeniería Social.
- ( ) b. Ataque de Fuerza utilizando Diccionarios.
- ( ) c. Spoofing. (Suplantación)
- ( ) d. Inyección SQL.
- ( ) e. Ataques de Cross-site scripting. (XSS)

Pregunta **5**

Finalizado

Puntúa 3,00 sobre 3,00

A qué tipo de ataque se refiere cuando un atacante logra inyectar un script hecho en JavaScript en las respuestas de una aplicación web de forma que se ejecuta en el navegador web del cliente y puede: robar cookies (sesiones) o redireccionar a otras páginas.

Seleccione una:

- ( ) a. Ataque de Fuerza utilizando Diccionarios.
- (•) b. Ataques de Cross-site scripting (XSS).
- ( ) c. Ingeniería Social.
- ( ) d. Spoofing. (Suplantación)
- ( ) e. Inyección SQL.

Pregunta **6**

Finalizado

Puntúa 3,00 sobre 3,00

La vulnerabilidad A1 Injection se genera cuando no se controla correctamente el input del usuario sobre la aplicación que se envía a un intérprete?

Seleccione una:

- Verdadero
- Falso

Pregunta **7**

Finalizado

Puntúa 3,00 sobre 3,00

Cual es la herramienta de prevención más efectiva contra ataques de Ingeniería social?

Seleccione una:

- a. Implementar políticas de complejidad contraseñas.
- b. Bloquear las Sesiones de las PCs cuando no se utiliza.
- c. Desarrollar un Programa de Concienciación de Seguridad de la información a Usuarios.
- d. Implementar Firewalls de perímetro.
- e. Utilizar OWASP como metodología de desarrollo Seguro.

Pregunta **8**

Finalizado

Puntúa 8,00 sobre 8,00

[OWASP] Tipos de A1 Injection que se pueden lograr? (Marque las respuestas correctas)

Seleccione una o más de una:

- a. Inyección SQL
- b. Inyección de parches
- c. Inyección LDAP
- d. Inyección de comandos de OS
- e. Inyección de códigos binarios

Pregunta **9**

Finalizado

Puntúa 4,00 sobre 4,00

Cuál de las siguientes acciones NO forma parte del proceso Detección de Vulnerabilidades y Análisis de Vulnerabilidades?

Seleccione una:

- a. Aplicación de Parches.
- b. Escaneo de Vulnerabilidades.
- c. Revisión de Reportes de proveedores.
- d. Revisiones de Seguridad.
- e. Suscripción a Boletines de Seguridad.

Pregunta **10**

Finalizado

Puntúa 0,00 sobre 3,00

De los siguientes actores quienes NO participan en la fase de "Priorización de Remediación Vulnerabilidades"

Seleccione una:

- a. Equipo de Gestión de Incidentes.
- b. Equipo Comercial o Productos.
- c. Equipo Gerencial.
- d. Clientes Corporativos.
- e. Equipo Técnico.

Pregunta **11**

Finalizado

Puntúa 0,00 sobre 2,00

¿Cual es el comando de NMAP que habilita la detección del Sistema Operativo?

Seleccione una:

- a. nmap -v -A scanme.nmap.org
- b. nmap -SO scanme.nmap.org
- c. nmap -O scanme.nmap.org
- d. nmap --script-trace scanme.nmap.org

Pregunta **12**

Finalizado

Puntúa 3,00 sobre 3,00

¿Cuándo se detecta una vulnerabilidad CRITICA (Según los criterios generales) en un Servidor de la infraestructura, como se define la Urgencia (Lenta/Rápida) para aplicar la remediación?

Seleccione una:

- a. Se aplica de manera rápida.
- b. Si es un sistema de criticidad ALTA para el negocio NO se aplica la remediación.
- c. Si es un servidor con Sistema Operativo Linux es Lenta.
- d. Se tiene en cuenta la criticidad del servidor para el negocio, cuanto más ALTA la remediación debe ser más Rápida.
- e. Se espera la recomendación oficial del proveedor.

Pregunta **13**

Finalizado

Puntúa 0,00 sobre 3,00

¿Cual es el comando de NMAP que nos permite ver si un host tiene vulnerabilidad de DOS.

Seleccione una:

- a.
nmap -O DOS scanme.nmap.org
- b. nmap -SO scanme.nmap.org
- c. nmap --script DOS scanme.nmap.org
- d. nmap -v -A –script ntest DOS scanme.nmap.org

Pregunta **14**

Finalizado

Puntúa 0,00 sobre 3,00

[OWASP] Mediante el TOP A6 de OWASP (Security Misconfiguration) se busca instalar el Sistema Operativo y el software utilizado para soportar la aplicación de forma segura?

Seleccione una:

- Verdadero
- Falso

Pregunta **15**

Finalizado

Puntúa 2,00 sobre 2,00

¿Cual es el comando de NMAP que nos permite chequear vulnerabilidades especificas de software y generan resultados solamente si dichas vulnerabilidades son encontradas?

Seleccione una:

- a.
  nmap -v -A –script external scanme.nmap.org
- b.
  nmap -SO vuln scanme.nmap.org
- c.
  nmap -O scanme.nmap.org
- d.
  nmap --script vuln scanme.nmap.org

◀ Trabajo Práctico - Vulnerabilidades

Ir a...

Evaluación del módulo y de los profesores ▶