recuperatorio 1er parcial

Total de puntos 39/40

✓ ¿ Cuál de los siguientes elementos no forma parte del OWASP Top-Ten? * 1/1

- ○ Redirecciones y reenvíos no validos
- ○ Configuración de seguridad Incorrecta
- ◉ Denegación de Servicio ✓
- ○ Referencia Directa Insegura A objetos

✓ Indique a que termino se asocia la siguiente definición: “[...] es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.” *1/1

- ○ Disponibilidad
- ◉ Integridad ✓
- ○ Confidencialidad
- ○ Consistencia

✓ ¿Qué es un firewall? * 1/1

- ◉ Un dispositivo que permite bloquear o filtrar el acceso entre dos redes. Usualmente privada y otra externa. ✓
- ○ Una librería de software que permite asegurar una aplicación web
- ○ Un dispositivo de antivirus de red
- ○ Un dispositivo que permite la autenticación de aplicaciones

✓ ¿En qué zona ubica al ataque de exposición de Datos Sensibles? * 1/1

- ○ Área de Red
- ○ Área de Servidor
- ○ Área de Red y Área de Servidor
- ◉ Área de Cliente ✓

✓ ¿Cuál de estas tecnologías es considerada generadora de riesgo por ser ejecutada en el lado del cliente? *1/1

- ○ ActiveX
- ○ Javascript
- ○ Java Applet
- ◉ Todas las anteriores ✓

✓ ¿A que se denomina “Learning Mode” en el contexto de la implementación de un WAF? *1/1

- ○ Ninguna de las anteriores
- ○ A la capacitación del personal que llevara adelante la configuración de la herramienta
- ◉ Al modo de operación donde la herramienta registra la actividad normal de la aplicación para que posteriormente pueda ser utilizada a fin de generar reglast ✓
- ○ Al modo de operación donde se permite que el usuario acceda a la aplicación para generar los ataque que posteriormente serán bloqueados

✗ SYN Flood corresponde a una técnica utilizada para realizar un ataque de ... *0/1

- (●) Inyección ✗
- ( ) Denegación de servicio
- ( ) Control remoto de un servidor
- ( ) Secuencia de Comandos de Sitios Cruzados (XSS)

Respuesta correcta

- (●) Denegación de servicio

✓ ¿Cuál de las siguientes tecnologías no puede ser utilizada en un ataque de inyección? *1/1

- ( ) LDAP
- ( ) SQL
- ( ) X-Patch
- (●) Ninguna ✓

✓ ¿Cuál de estas afirmaciones es verdadera en relación a los Firewalls? * 1/1

- (●) Todas las anteriores ✓
- ( ) No protege de todos los ataques dañinos
- ( ) No protege de accesos no autorizados
- ( ) No protege de ataques internos

✓ ¿Qué protocolo soporta la implementación de VPNs? * 1/1

- (●) IPSec ✓
- ( ) ICMP
- ( ) Ninguna de las opciones
- ( ) Secure TCP

✓ ¿Qué es un bugtraq? * 1/1

- ( ) Es una variante de virus o troyano
- (●) Es una lista de notificación sobre vulnerabilidades encontradas en un software y hardware ✓
- ( ) Es un software diseñado para buscar vulnerabilidades
- ( ) Ninguna de las opciones es correcta

✓ ¿Qué se entiende por “tampering”? * 1/1

- (●) Es un ataque de alteración de datos no autorizados ✓
- ( ) Ninguna respuesta es correcta
- ( ) Es una vulnerabilidad que afecta al código javascript
- ( ) Es una técnica para redireccionar al usuario hacia otro servidor

✓ ¿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.” *1/1

- ○ Statefull
- ○ HoneyNets
- ○ HonetPosts
- ◉ IDS ✓

✓ ¿Cuál de los siguientes elementos corresponde a una Modalidad de Acceso a la información de Seguridad Lógica? *1/1

- ○ Borrado
- ○ Lectura
- ◉ Todas las opciones ✓
- ○ Escritura
- ○ Ejecución

✓ ¿Cuál de las siguientes opciones corresponde al modelo de funcionamiento general de un IDS? *1/1

- ○ Recolección – Identificación – Clasificación
- ○ Ninguno de los anteriores
- ◉ Recolección – Análisis – Respuesta ✓
- ○ Filtrado – Identificación – Acción

✓ ¿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 puertos” *1/1

- ○ Router
- ◉ Switch ✓
- ○ Hub
- ○ Bridge

✓ ¿Cuál de los siguientes elementos no compone la lista de técnicas de OWASP TopTen Proactive Controls? *1/1

- ○ Validate All Inputs
- ○ Encode Data
- ○ Implement Appropiate Access Controls
- ◉ Use Virtual Keyboard in the Login ✓
- ○ Parameterize Queries

✓ 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” *1/1

- ○ Falsificación de peticiones en sitios cruzados (CSRF)
- ○ Referencia directa insegura a objetos
- ○ Inyección
- ◉ XSS – Cross Site Scriping ✓

✓ 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." *1/1

- ○ Referencia directa insegura a objetos
- ○ Falsificación de peticiones en sitios cruzados (CSRF)
- ○ Perdida de autenticación y gestión de sesiones
- ◉ Inyección ✓

✓ ¿Cuál de los siguientes tipos NO corresponde a la lista OWASP de 10 ataques más frecuentes? *1/1

- ○ Inyección
- ○ Falsificación de peticiones en sitios cruzados (CSRF)
- ◉ Control de accesos sin contraseña seguras ✓
- ○ Perdida de autentificación y gestión de sesión

✓ ¿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."? *1/1

- ○ Falsificación de Peticiones en Sitios Cruzados (CSRF)
- ○ Referencia Directa Insegura a Objetos
- ○ Ausencia de Control de Acceso a Funciones
- ◉ Secuencia de Comandos en Sitios Cruzados (XSS) ✓

✓ ¿Cuál de las siguientes características no están asociadas a los Firewalls? *1/1

- ○ Balanceo de carga (BCFW)
- ○ Alta disponibilidad (AD)
- ○ Filtrados de contenido / Anti-Spam
- ◉ Almacenamiento de datos de negocio ✓

✓ ¿Cuál de los siguientes elementos NO esta catalogado como una Acción Hostil en Seguridad Física? *1/1

- ○ Fraude
- ○ Robo
- ◉ Inundación ✓
- ○ Sabotaje

✓ ¿Cuál de los siguientes elementos NO forma parte de la pirámide ID? * 1/1

- Ninguno
- Disponibilidad
- Confidencialidad
- Identificación ✓

✓ ¿Cuál de los siguientes elementos NO se encuentra dentro de los Controles de Acceso Interno de la seguridad lógica? *1/1

- Ninguno ✓
- Lista de control de acceso
- Etiquetas de seguridad
- Constraseñas

✓ Seleccione la opción según la definición de amenaza: “Entendemos como amenaza aquella situación de daño cuyo…” *1/1

- Origen se encuentra en el código de la aplicación
- Impacto genera una detención total del sistema
- Impacto no afecta a la funcionalidad del sistema
- Riesgo de producirse es significativo ✓

✓ ¿Cuál de los siguientes puntos NO es un atributo del protocolo TCP? * 1/1

- (●) No es orientado a conexión ✓
- ( ) Corre sobre IP
- ( ) Un paquete tiene un numero de puerto origen y destino
- ( ) Cada paquete tiene un numero de secuencia y un flag

✓ ¿Cuál de los siguientes elementos se utiliza con el fin de capturar tramas de red? *1/1

- ( ) IDS
- ( ) Firewall Personal
- ( ) Ninguno de los anteriores
- (●) Sniffer ✓

✓ ¿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.)? *1/1

- (●) DMZ ✓
- ( ) B2B
- ( ) Router
- ( ) LBA

✓ ¿En que zona ubica al ataque de Inyección? * 1/1

- Area de Red
- D. Ninguna
- Area de Cliente
- Area de servidor ✓

✓ ¿Cual de los siguientes puntos NO corresponde a un tipo de vulnerabilidad? *1/1

- Debidas al diseño
- Ninguna de las anteriores ✓
- Debidas al uso
- Debidas a la implementacion

✓ ¿Cual de los siguientes factores no es evaluado por la OWASP para determinar los riesgos incluidos en el proyecto Top-Ten? *1/1

- Detectabilidad de debilidades
- Impacto tecnico
- Impacto en el negocio ✓
- Vectores de ataque

✓ ¿Cual es la principal funcion de un comprobador de integridad? * 1/1

- ○ Notificar via email sobre cambios en el sistema de archivos
- ○ Identificar al usuario que ha introducido cambios en el sistema de archivos
- ◉ Identificar archivos que han sido alterados en el sistema de archivos ✓
- ○ Identificar los cambios realizados en los archivos del sistema

✓ Seleccione el tipo de ataque correspondiente a la siguiente definicion: "es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legitimos" *1/1

- ○ Tampering
- ○ Inyeccion
- ○ Perdida de autenticacion
- ◉ Denegacion de servicio ✓

✓ ¿Cual de estos elementos corresponde a la siguiente definicion: "Se trata de un dispositivo que analiza el trafico web (entre el servidor web y la WAN), los datos recibidos por parte del usuario y protege de diferentes ataques"? *1/1

- ◉ WAF ✓
- ○ Firewall personal
- ○ IDS
- ○ Layer 3 Firewall

✓ Segun la definicion de "Daño" selecciona la respuesta correcta: * 1/1

- ○ Se debe expresar en probabilidad de ocurrencia
- ◉ Debe ser cuantificable ✓
- ○ Ocurre solo cuando se inhabilita el sistema de forma completa
- ○ Todas las respuestas son correctas

✓ La seguridad de informacion comprende: * 1/1

- ◉ Analisis de Riesgo / Normativas / Plan Director ✓
- ○ Analisis de Riesgo / Auditoria de Eventos / Normativas
- ○ Normativas / Tecnicas de Proteccion / Plan Director
- ○ Plan Director / Configuracion segura / Auditoria de Eventos

✓ ¿Cual es el conjunto de estandares que nos permite asignar a las vulnerabilidades una valoracion numerica entre 0.0 y 10.0 ? *1/1

- ○ TopTen
- ◉ CVSS ✓
- ○ CWE
- ○ CVE

✓ La seguridad informatica se encarga de: * 1/1

- ○ Desarrollar politicas y procedimientos de seguridad de la informacion
- ◉ Implementar tecnologias de proteccion de la informacion, como antivirus, firewalls, etc. ✓
- ○ Analizar los riesgos y amenazas a la informacion
- ○ Asegurar la confidencialidad, integridad, disponibilidad de la informacion

✓ La seguridad de la informacion se encarga de: * 1/1

- ○ Analizar los riesgos y amenazas a la información.
- ○ Implementar tecnologías de protección de la información, como antivirus, firewalls, etc.
- ○ Desarrollar políticas y procedimientos de seguridad de la información.
- ◉ Asegurar la confidencialidad, integridad y disponibilidad de la información. ✓