Examen para HE01.

Intento 1

Pregunta 1

¿Qué es el estándar CVSS?:

a. Un estándar para la medir la criticidad de una vulnerabilidad.
b. Un estándar para medir la superficie de ataque.
c. Un framework de trabajo que nos indica el tipo de vulnerabilidades a comprobar en una auditoría.
d. Un estándar de calidad.

Pregunta 2

Indica cuál de las siguientes afirmaciones es correcta:

a. Una auditoría que haga uso de pruebas automáticas va a localizar las mismas vulnerabilidades que se localizarían en una auditoría con pruebas manuales.
b. El objetivo de los test de intrusión es llegar a comprometer un sistema a través de una vulnerabilidad.
c. En los test de intrusión únicamente se confirman vulnerabilidades.
d. Las auditorías de tipo automático no generan muchos falsos positivos.

Pregunta 3

Indica cuál de las siguientes herramientas es utilizada para automatizar la búsqueda de vectores de elevación de privilegios en sistemas Linux:

a. PrivescCheck.
b. LinPEAS.
c. LinescCheck.
d. WinPeas.

Pregunta 4

Indica cual es la afirmación correcta:

a. El mecanismo utilizado para medir la criticidad de las vulnerabilidades se realiza según el criterio del auditor.
b. Los roles dedicados a la gestión se apoyan en el informe ejecutivo para interpretar los riesgos de la vulnerabilidad.
c. El informe técnico detalla los pasos de como explotar una vulnerabilidad, pero no su resolución.
d. Los roles dedicados a la gestión se apoyan en el informe técnico de auditoría para tomar decisiones.

Pregunta 5

La herramienta nmap puede utilizarse para realizar un escaneo de vulnerabilidades.
¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 6

Indica cuál de las siguientes herramientas se utilizan para realizar técnicas de fuerza bruta de credenciales:

a. Hydra
b. Wireshark
c. Echo mirage
d. goPhish

Pregunta 7

Indica cuál de las siguientes opciones NO pertenece a la Fase de "Seguimiento de las pruebas":

a. Se comunicarán todas las vulnerabilidades detectadas y se procederá al cierre de la auditoría.
b. Se comunicarán al cliente los hallazgos localizados desde la reunión anterior.
c. Se comunicarán los problemas que pudieran haber surgido desde la reunión anterior.
d. Se decidirá en qué activos o secciones incrementar el esfuerzo en las próximas semanas.

Pregunta 8

Indica cuál de las siguientes afirmaciones NO es correcta para una auditoría de tipo "Test de intrusión":

a. Las pruebas se realizan por un auditor de manera manual apoyándose en herramientas específicas. También se contempla el uso de sistemas secundarios para ciertos tipos de pruebas.
b. Tratan de comprometer el sistema remoto a través de una vulnerabilidad identificada.
c. Debido a la forma en la que se detectan las vulnerabilidades, se producen muchos falsos positivos
d. Tienen como objetivo comprobar el grado real de amenaza que podría producirse al aprovecharse de las vulnerabilidades localizadas durante la auditoría y verificar el impacto específico que tendrían sobre la compañía

Pregunta 9

Las herramientas de tipo keylogger se ejecutan en una máquina comprometida para capturar todas las pulsaciones de teclado. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 10

En las auditorías manuales NO se pueden utilizar herramientas automáticas. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Intento 2

Pregunta 1

Durante la presentación de resultados únicamente se presentan los resultados de la auditoría, pero no se resuelven dudas ni se dan recomendaciones para solventar las vulnerabilidades. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 2

¿Cuál de las siguientes labores de la fase de Pre-engagement NO es una labor organizativa?:

a. Identificar el entorno y enfoque de las pruebas.
b. Establecer un canal de comunicación para las incidencias graves.
c. Delimitar el alcance de la auditoría.
d. Designar personas de contacto durante el tiempo de auditoría.

Pregunta 3

Indica cuál de las siguientes afirmaciones es correcta para una auditoría con pruebas de caja blanca:

a. Se puede disponer del código fuente del aplicativo a auditar para poder localizar vulnerabilidades en código.
b. Las pruebas se realizan sin ningún tipo de conocimiento sobre la aplicación o infraestructura a auditar.
c. No se dispone de tecnologías utilizadas, frameworks o lenguajes de programación utilizados, diagramas de red o de flujo, etc.
d. En este tipo de pruebas si se contempla que puedes partir de uno, varios usuarios iniciales o, que por el contrario, no dispongas de ningún usuario al iniciar las pruebas.

Pregunta 4

Indica cuál de las siguientes opciones es una afirmación correcta para la Fase de Explotación:

a. Se recopila información acerca de los activos a auditar.
b. Se detectan vulnerabilidades que puedan existir en los sistemas y servicios
c. El objetivo es lograr un primer acceso o de privilegios en los activos.
d. Se utilizan técnicas para poder aumentar el nivel de privilegios en este sistema.

Pregunta 5

¿Cuál es la definición del término “Vulnerabilidad”?:

a. Es una debilidad que puede ser explotada con la materialización de una o varias amenazas a un activo.
b. Es un objeto o recurso de valor (tangible o intangible) empleado en una empresa u organización. Cuya pérdida o daño constituiría un riesgo para la organización.
c. Es un evento que puede causar un incidente de seguridad en una empresa u organización produciendo pérdidas o daños potenciales en sus activos.
d. Es un activo que puede disponer de una o varias amenazas.

Pregunta 6

En las pruebas de caja negra nunca se proporcionan usuarios de acceso al activo a auditar. ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 7

¿Cuál de las siguientes técnicas no forma parte de la fase de reconocimiento activo?:

a. Enumeración SNMP.
b. Enumeración SMB (o enumeración NetBIOS).
c. Enumeración SMTP.
d. Búsqueda de información en redes sociales.

Pregunta 8

¿Cuáles son los tres pilares de la seguridad de la información?:

a. Confidencialidad, identidad y disponibilidad.
b. Responsabilidad, integridad y disponibilidad.
c. Confidencialidad, integridad y disponibilidad.
d. Confidencialidad, integridad y seguridad.

Pregunta 9

¿Qué es la DarkWeb?:

a. Todo el contenido privado que no se encuentra a disposición del público en general.
b. Redes privadas utilizadas por los ciberdelincuentes para ofrecer sus servicios, vender información previamente robada, vulnerabilidades no reportadas a los fabricantes.
c. Contenido utilizado por los ciberdelincuentes pero que se encuentra disponible de manera pública en internet.
d. Contenido que se encuentra disponible de manera pública en internet.

Pregunta 10

¿Cuál de las siguientes herramientas se utilizan en un Reconocimiento pasivo?:

a. snmpwalk.
b. shodan.
c. nmap.
d. dig.