Seguridad en Redes y Sistemas de Software

Comenzado en	Thursday, 24 de September de 2020, 08:07
Estado	Terminado
Finalizado en	Thursday, 24 de September de 2020, 08:42
Tiempo empleado	34 minutos 24 segundos
Puntos	53.00/53.00
Calificación	**10.00** de un total de 10.00 (**100**%)

Pregunta **1**
Correcta
Puntúa 6.00 sobre 6.00
Señalar con bandera la pregunta

Las siguientes deficiones, tienen que ver con la terminología escencial, relaciona correctamente:

Activo	Algo de valor que utiliza la empresa para cumplir sus objetivos de negocio	✓
Riesgo	Es la probabilidad de que ocurra un incidente no indeseado que afecte negativamente a la organización	✓
Amenaza	Cualquier cosa que pueda explotar una vulnerabilidad para comprometer un activo	✓
Controles	Acciones llevadas a cabo para mitigar efectivamente las amenazas	✓
Impacto	Magnitud de las consecuencias para el negocio	✓
Vulnerabilidad	Una debilidad o brecha en nuestros controles de seguridad	✓

La respuesta correcta es: Activo → Algo de valor que utiliza la empresa para cumplir sus objetivos de negocio, Riesgo → Es la probabilidad de que ocurra un incidente no indeseado que afecte negativamente a la organización, Amenaza → Cualquier cosa que pueda explotar una vulnerabilidad para comprometer un activo, Controles → Acciones llevadas a cabo para mitigar efectivamente las amenazas, Impacto → Magnitud de las consecuencias para el negocio, Vulnerabilidad → Una debilidad o brecha en nuestros controles de seguridad

Pregunta **2**
Correcta
Puntúa 5.00 sobre 5.00
Señalar con bandera la pregunta

Las siguientes son las fases de hacking ético, relaciona correctamente:

Reconocimiento	Se refiere a la fase preparatoria donde un atacante busca obtener la mayor cantidad de información como sea posible ac	✓
Mantener acceso	Se refiere a la fase cuando el atacante trata de retener su propiedad sobre el sistema	✓
Escaneo	Se refiere a la fase de pre ataque cuando el hacker escanea la red en busca de información específica en base a la inform	✓
Ganar acceso	Se refiere al punto donde el atacante obtiene acceso al sistema operativo o a las aplicaciones de la computadora o sister	✓
Cubrir o borrar huellas	Se refiere a las actividades que el hacker emprende para esconder sus fechorias.	✓

Su respuesta es correcta.

La respuesta correcta es: Reconocimiento → Se refiere a la fase preparatoria donde un atacante busca obtener la mayor cantidad de información como sea posible acerca del objetivo en evaluación previo al lanzamiento de un ataque., Mantener acceso → Se refiere a la fase cuando el atacante trata de retener su propiedad sobre el sistema, Escaneo → Se refiere a la fase de pre ataque cuando el hacker escanea la red en busca de información específica en base a la información obtenida durante el reconocimiento., Ganar acceso → Se refiere al punto donde el atacante obtiene acceso al sistema operativo o a las aplicaciones de la computadora o sistema., Cubrir o borrar huellas → Se refiere a las actividades que el hacker emprende para esconder sus fechorias.

Pregunta **3**
Correcta
Puntúa 3.00 sobre 3.00
Señalar con bandera la pregunta

Las siguientes son las "Clases de Hackers", relaciona correctamente:

Black Hats	Individuos con capacidades de computo extraordinarias, dedicados a actividades maliciosas o destructivas. También conocidos con	✓
White Hats	Individuos profesando habilidades de hacker y usándolas para propósitos defensivos. También conocidos como analistas de seguri	✓
Gray Hats	Individuos que trabajan de ambos lados ofensivamente y defensivamente en varios momentos del tiempo.	✓

La respuesta correcta es: Black Hats → Individuos con capacidades de computo extraordinarias, dedicados a actividades maliciosas o destructivas. También conocidos como crackers., White Hats → Individuos profesando habilidades de hacker y usándolas para propósitos defensivos. También conocidos como analistas de seguridad., Gray Hats → Individuos que trabajan de ambos lados ofensivamente y defensivamente en varios momentos del tiempo.

Pregunta **4**
Correcta
Puntúa 3.00 sobre 3.00
Señalar con bandera la pregunta

Se refiere a las diferente formas de efectuar pruebas de seguridad (pruebas de penetración), relaciona correctamente:

Gray-Box	Llevar a cabo una auditoria interna utilizando los permisos otorgados a los miembros de la empresa.	✓
Black-Box	Evaluar la red como si no se tuviera conocimientos previos de ella.	✓
White-Box	Evaluar la red teniendo un conocimiento pleno de la los objetivos a evaluar.	✓

La respuesta correcta es:
Gray-Box
→ Llevar a cabo una auditoria interna utilizando los permisos otorgados a los miembros de la empresa.,
Black-Box
→ Evaluar la red como si no se tuviera conocimientos previos de ella., White-Box → Evaluar la red teniendo un conocimiento pleno de la los objetivos a evaluar.

Pregunta **5**
Correcta
Puntúa 5.00 sobre 5.00
Señalar con bandera la pregunta

Las siguientes, son algunas leyes mexicanas que tienen que ver con la informática y la seguridad, realaciona correctamente:

Ley de la Propiedad Industrial	Esta tiene como objeto proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de inven	✓
Ley Federal de Telecomunicaciones	Esta tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telec	✓
Ley Federal del Derecho de Autor	Esta ley contempla principalmente los derechos patrimoniales sobre un programa de computación y su documentaci	✓
Código penal federal	Castiga el Acceso Ilícito a Sistemas y Equipos de Informática, Art. 211, bis1 al bis 5	✓
Ley de Información Estadística y Geográfica	Su objetivo es normar el funcionamiento de los Servicios Nacionales de Estadística y de Información Geográfica y reg	✓

La respuesta correcta es: Ley de la Propiedad Industrial
→ Esta tiene como objeto proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales, marcas y avisos comerciales; publicación de nombres comerciales .., Ley Federal de Telecomunicaciones → Esta tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, y de la comunicación vía satélite.,
Ley Federal del Derecho de Autor
→ Esta ley contempla principalmente los derechos patrimoniales sobre un programa de computación y su documentación, copias autorizadas y la protección de uso de las bases de datos así como el acceso a información privada., Código penal federal → Castiga el Acceso Ilícito a Sistemas y Equipos de Informática, Art. 211, bis1 al bis 5,
Ley de Información Estadística y Geográfica
→ Su objetivo es normar el funcionamiento de los Servicios Nacionales de Estadística y de Información Geográfica y regular el desarrollo y la utilización permanente de la informática en los servicios nacionales referentes a los servicios citados.

Pregunta **6**
Correcta
Puntúa 5.00 sobre 5.00
Señalar con bandera la pregunta

Las siguientes son las diferentes áreas en las que se basa un Concurso CTF tipo Jeopardy, y de las cuales se debe tener nociones generales para poder considerarse con buenos fundamentos de seguridad, relaciona correctamente:

Entender las matemáticas asociadas a los algoritmos criptográficos con el fin detectar debilidades en su implementación y así descifrar el código.	Crypto	✓
Entender las vulnerabilidades asociadas a los lenguajes de programación web explotarlas y obtener algún tipo de acceso privilegiado. De igual forma entender los protcolos de Internet que tienen que ver con el web.	Web	✓
Convertir un archivo binario a lenguaje ensamblador (desensablado) para comprender la funcionalidad del mismo a fin de detectar posibles fallas.	Reversing	✓
Explotar un archivo binario con a finalidad de obtener una shell, haciendo un desensamblado del mismo para encontrar vulnerabilidades. En muchas ocasiones el binario es un servicio que corre de forma remota en un servidor y al explotarlo nos da acceso al mismo.	Pwning	✓
Encontrar datos eliminados, no almacenados o encubiertos. Se debe comprender perfectamente como se construyen los datos para su análisis.	Forensic	✓

Su respuesta es correcta.

La respuesta correcta es: Entender las matemáticas asociadas a los algoritmos criptográficos con el fin detectar debilidades en su implementación y así descifrar el código.

→ Crypto, Entender las vulnerabilidades asociadas a los lenguajes de programación web explotarlas y obtener algún tipo de acceso privilegiado. De igual forma entender los protcolos de Internet que tienen que ver con el web. → Web, Convertir un archivo binario a lenguaje ensamblador (desensablado) para comprender la funcionalidad del mismo a fin de detectar posibles fallas. → Reversing, Explotar un archivo binario con a finalidad de obtener una shell, haciendo un desensamblado del mismo para encontrar vulnerabilidades. En muchas ocasiones el binario es un servicio que corre de forma remota en un servidor y al explotarlo nos da acceso al mismo. → Pwning, Encontrar datos eliminados, no almacenados o encubiertos. Se debe comprender perfectamente como se construyen los datos para su análisis. → Forensic

Pregunta **7**
Correcta
Puntúa 12.00 sobre 12.00
Señalar con bandera la pregunta

Los siguientes son algunos comandos básicos utilizados en Linux y que usamos en las prácticas de Retos Bandit , relaciona correctamente.

openssl s_client	Permite conectarse a un servidor remoto SSL creando un canal encriptado	✓
Permite mostrar el contenido de un archivo con espacios en el nombre	cat "nombre del archivo con espacios"	✓
strings	Permite exttraer las cadenas de texto de un archivo binario	✓
grep	Permite filtrar líneas de texto en base a un patrón	✓
uniq	Permite contar las ocurrencias o mostrar líneas en un archivo de texto	✓
Permite mostrar el contenido del archivo	cat archivo	✓
base64	Permite codificar / decodificar cadenas en codificación base64	✓
Permite ver que tipo de archivos son los todos archivos de la carpeta actual	file ./*	✓
Permite obtener un listado extendido de los de archivos en el directorio actual	ls -la	✓
Permite localizar un archivo dentro del sistema (en base al tipo, tamaño y usuario propietario del archivo)	find -type f -size 1033c -user bandit4	✓
Permite conectarse a un servidor remoto a un puerto especifico	nc remotehost 3045	✓
sort	Permite ordenar lineas de texto	✓

Su respuesta es correcta.

La respuesta correcta es: openssl s_client → Permite conectarse a un servidor remoto SSL creando un canal encriptado, Permite mostrar el contenido de un archivo con espacios en el nombre → cat "nombre del archivo con espacios", strings → Permite exttraer las cadenas de texto de un archivo binario, grep → Permite filtrar líneas de texto en base a un patrón, uniq → Permite contar las ocurrencias o mostrar líneas en un archivo de texto, Permite mostrar el contenido del archivo → cat archivo, base64 → Permite codificar / decodificar cadenas en codificación base64, Permite ver que tipo de archivos son los todos archivos de la carpeta actual → file ./*, Permite obtener un listado extendido de los de archivos en el directorio actual → ls -la, Permite localizar un archivo dentro del sistema (en base al tipo, tamaño y usuario propietario del archivo) → find -type f -size 1033c -user bandit4, Permite conectarse a un servidor remoto a un puerto especifico → nc remotehost 3045, sort → Permite ordenar lineas de texto

Pregunta **8**
Correcta
Puntúa 6.00 sobre 6.00
Señalar con bandera la pregunta

Son comandos de Linux utilizados para "Información del Sistema y Manejo de Procesos", relacione correctamente:

ps aux	Muestra todos los procesos del sistema	✓
ps -all	Muestra todos los procesos del usuario	✓
uptime	Muestra el tiempo que lleva encendido el sistema	✓
pkill proc	Mata el proceso llamado "proc"	✓
uname -a	Despliega información del sistema de Linux	✓
whoami	Muestra el usuario que se encuentra logueado	✓

Su respuesta es correcta.

La respuesta correcta es: ps aux → Muestra todos los procesos del sistema, ps -all → Muestra todos los procesos del usuario, uptime → Muestra el tiempo que lleva encendido el sistema, pkill proc → Mata el proceso llamado "proc", uname -a → Despliega información del sistema de Linux, whoami → Muestra el usuario que se encuentra logueado

Pregunta **9**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

Los siguientes, son los "elementos de la seguridad de la información" que se deben garantizar:

Seleccione una:
- ○ a. Reconocimiento, escaneo, ganar acceso, mantener acceso, borrar hueyas
- ● b. Confidencialidad, integridad y disponibilidad ✓
- ○ c. Politicas, incidentes, procedimientos, consientización

La respuesta correcta es: Confidencialidad, integridad y disponibilidad

Pregunta **10**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

Son las fases del hacking ético en su orden correcto:

Seleccione una:
- ● a. Reconocimiento, escaneo, ganar acceso, mantener acceso, borrar huellas ✓
- ○ b. Black hat, grey hat, white hat
- ○ c. White hat, grey hat, black hat
- ○ d. Borrar huellas, mantener acceso, ganar acceso, escaneo, reconocimiento

Su respuesta es correcta.

La respuesta correcta es: Reconocimiento, escaneo, ganar acceso, mantener acceso, borrar huellas

Pregunta **11**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

Son los diferentes tipos de concursos CTF que existen y que se pueden utilizar para aprender seguridad de la información y hacking ético de manera legal:

Seleccione una:
- ○ a. Reconocimiento, Escaneo, Ganar Acceso, Mantener Acceso, Borrar Huellas
- ● b. Jeopardy, Attack/Defense, Boot to root, Wargames ✓
- ○ c. Black Hat, Grey Hat, White Hat

Su respuesta es correcta.

La respuesta correcta es: Jeopardy, Attack/Defense, Boot to root, Wargames

Pregunta **12**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

La investigacion de vulnerabilida ✓ consiste en descubrir vulnerabilidades y debilidades de diseño que abrirán un sistema operativo y sus aplicaciones a un ataque o mal uso. Incluye tanto el estudio dinámico de productos y tecnologías como seguimiento del mundo hacker alterno (underground).

La respuesta correcta es: investigacion de vulnerabilidades

Pregunta **13**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

Un red team ✓ es un enfoque donde un grupo de hackers éticos lleva a cabo pruebas de penetración en los sistemas de información sin acceso o un acceso muy limitado a los recursos internos de la organización. Esta prueba puede efectuarse con o sin una advertencia previa. Este tipo de prueba es propuesta para detectar vulnerabilidades de red y de sistema y revisar la seguridad desde la perspectiva del atacante a la red, sistemas, o activos de información

La respuesta correcta es: red team

Pregunta **14**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

La ley federal de proteccion de datos personales en ✓ tiene por objeto proteger los datos persoonales con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

La respuesta correcta es: ley federal de proteccion de datos personales en manos de particulares

Pregunta **15**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

La Seguridad de la Información consiste en : proteger la confidencialidad, integridad, y disponibilidad de los activos de información, ya sea en el almacenamiento, procesamiento o trasmisión, a través de la aplicación de políticas, educación, entrenamiento / concientización, y tecnología ?

Elija una;
- ● Verdadero ✓
- ○ Falso

La respuesta apropiada es 'Verdadero

Pregunta **16**
Correcta
Puntúa 1.00 sobre 1.00
Señalar con bandera la pregunta

El hacking ético involucra el uso de herramientas de hacking, trucos y técnicas para explotar vulnerabilidades , ganar acceso no autorizado al sistema y beneficiarse con la información obtenida.

Elija una;
- ○ Verdadero
- ● Falso ✓

La respuesta apropiada es 'Falso

Navegación dentro del examen

1 ✓ 2 ✓ 3 ✓ 4 ✓ 5 ✓ 6 ✓ 7 ✓ 8 ✓ 9 ✓
10 ✓ 11 ✓ 12 ✓ 13 ✓ 14 ✓ 15 ✓ 16 ✓

Mostrar una página cada vez

Finalizar revisión

◄ Participa CTF 05 - Retos bandit 20 al 25

Ir a... ▾

Finalizar revisión