EXAMEN PARCIAL DE SEGURIDAD INFORMÁTICA

Alumno: Larreategui Castro, Angel Vidal
Código: 20171385I
Fecha: 31/10/2021
Profesor: Sidney Valer Quispe

1) Usted como especialista en seguridad informática de una empresa tiene la responsabilidad de asesorar en materia de seguridad. Su principal interés en capacitar a los empleados de la empresa es el tema de concienciación de seguridad porque deben defenderse de.
   a) La denegación de servicio
   b) El malware
   c) Ingeniería social
   d) Botnets

   Al conjunto de técnicas para engañar a los usuarios poco experimentados para que envíen sus datos personales, confidenciales, infectar sus PC con malwares o que puedan abrir enlaces a sitios web infectados que usan los cibercriminales se le denomina ingeniería social.

2) ¿Qué protocolo de configuración de red es utilizado para proporciona información de configuración a los hosts en redes, en particular las direcciones IP de los resolutores DNS de caché locales, los servidores de arranque de red y otros hosts de servicio?
   a) DHCP (Dynamic Host Configuration Protocol)
   b) NIS (Network Information Service)
   c) DNS (Domain Name Service)
   d) LDAP (Lightweight Directory Access Protocol)

   DHCP significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales. También asigna la máscara de subred, la dirección de puerta de enlace predeterminada, la dirección del servidor de nombres de dominio (DNS) y otros parámetros de configuración pertinentes.

3) ¿Cuál de las siguientes es la secuencia correcta de las capas del modelo de interconexión de sistemas abiertos (OSI), empezando por la capa más cercana al usuario final?
   a) Aplicación, sesión, red y física
   b) Aplicación, red, sesión y física
   c) Presentación, red, transporte y físico
   d) Transporte, presentación, red y físico

   La secuencia correcta de las capas del modelo OSI es aplicación, seguido dela sesión, red y física.

4) ¿Cómo se puede prevenir una vulnerabilidad de desbordamiento de **búfer**?
   a) Utilizando listas negras que contengan todos los caracteres que puedan ser potencialmente dañinos y no permitiéndolos en la función
   b) Instalando parches para corregir las vulnerabilidades de desbordamiento del búfer
   c) Programando con C++ en lugar de C porque C++ no es vulnerable a los desbordamientos de búfer como C

d) Utilizando lenguajes de programación fuertemente tipados, implementando la comprobación de límites y entradas, y utilizando funciones de almacenamiento

Un búfer es un espacio de memoria en el que se almacenan datos evitando que el programa que los necesita se quede sin datos durante una transferencia. Los datos son almacenados en un buffer mientras se transfieren desde un dispositivo de entrada o antes de enviarlos a un dispositivo de salida. También puede utilizarse para transferir datos entre procesos.

5) Un control eficaz contra los **ataques de inyección** en lenguaje de consulta estructurado (SQL) es
   a) Implementar un software antivirus
   b) Validar el ingreso de datos del usuario
   c) Cifrar las comunicaciones utilizando la **seguridad de la capa de transporte (TLS)**
   d) Desplegar un sistema de prevención de intrusiones

Seguridad de la capa de transporte y su antecesor Secure Sockets Layer son protocolos criptográficos, que proporcionan comunicaciones seguras por una red, comúnmente Internet.

La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios. Le explicamos cómo funcionan los ataques de inyección de SQL, cómo combatirlos y cómo una herramienta antivirus potente lo puede proteger contra las consecuencias.

6) Cinco (5) ejemplos de soluciones exitosas para evitar el robo incluyen
   a) Estrictos controles de acceso, sistemas de detección de intrusos, puertos bloqueados, control de claves y control de bag
   b) Estrictos controles de acceso, software antiphishing, puertos bloqueados, control de claves y control de bag
   c) Identificación y autenticación, sistemas de detección de intrusos, puertos bloqueados, control de claves y comprobación de bag
   d) Identificación y autenticación, software antiphishing, puertos bloqueados, control de claves y comprobación de bag

La identificación es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema. La autenticación es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.

7) ¿Cuál es el papel del auditor?
   a) El auditor comprueba la eficacia de los controles implementados por la organización en términos de diseño, aplicación y realiza los cambios necesarios
   b) El auditor se asegura que los controles cumplen con el COBIT (Objetivos de Control para TI)
   c) El auditor comprueba que los controles cumplen con la **norma ISO (Organización Internacional de Normalización) 27001**:2005, Anexo A (Sección de Controles)
   d) El auditor compara la política declarada con los controles reales existentes

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

8) La persona con la mayor responsabilidad para establecer los niveles de clasificación y el cumplimiento de los controles de acceso de cada activo de información sensible es el
   a) El responsable local
   b) Auditor
   c) Propietario de la información
   d) Individuo

   Según ISO 27001 sería el propietario de la información.

9) ¿Cuáles son las tres (3) categorías de la informática forense?
   a) Investigación de medios, tráfico de red y software
   b) Investigación de datos, procesos y sistemas informáticos
   c) Investigación de datos, sistemas y personas
   d) Investigación de la escena del crimen, las pruebas y los sospechosos

   Las categorías de la informática forense son la investigación de datos, los procesos y los sistemas informáticos.

10) Si hay registros históricos almacenados en el servidor que son extremadamente importantes para la empresa y que nunca deben ser modificados. Le gustaría añadir un control de integridad que le permita verificar periódicamente que los archivos no han sido modificados. ¿Qué control puede añadir?
   a) Hashing
   b) ACLs
   c) Atributos de sólo lectura
   d) Firewall

   El hashing se refiere al proceso de generar un output de extensión fija, a partir de un input de extensión variable. Esto se logra mediante el uso de unas fórmulas matemáticas denominadas funciones hash.

11) El administrador de red comienza a experimentar síntomas de lentitud. Al investigar, se da cuenta que la red está siendo bombardeada con paquetes **TCP SYN** y cree que su organización es víctima de un ataque de denegación de servicio. ¿Qué principio de seguridad de la información se está se está violando?
   a) Disponibilidad
   b) Integridad
   c) Confidencialidad
   d) Negación

   TCP SYN es un tipo de ataque de denegación de servicio (DoS) o denegación de servicio distribuido (DDoS) que envía un número masivo de solicitudes SYN a un servidor para sobrepasar su capacidad con conexiones abiertas.

12) ¿Cuál es el último paso de un análisis cuantitativo del riesgo?
   a) Determinar el valor de los activos.

b) Evaluar la tasa de ocurrencia anualizada.
c) Derivar la expectativa de pérdida anualizada.
d) Realizar un análisis coste/beneficio.

Al realizar un análisis de coste/beneficio se podrá calcular cuanto es la pérdida que se obtiene por estos errores y cuanto sería el beneficio si estos se arreglan.

13) Andrea está diseñando el plan de seguridad a largo plazo para su organización y tiene un horizonte de planificación de tres a cinco años. ¿Qué tipo de plan está desarrollando?
a) Operativo
b) Táctico
c) Resumen
d) Estratégico

Al desarrollar un plan de seguridad a largo plazo está diseñando un plan estratégico.

14) ¿Cuál de las siguientes alternativas es el proceso de identificar, reducir los riesgos a niveles controlables y luego implementar controles para mantener los riesgos en ese nivel?
a) Retorno de la inversión
b) Riesgo
c) Análisis de riesgos
d) Gestión de riesgos

La gestión del riesgo se define como el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse.

15) ¿Cuáles de las siguientes alternativas son las mejores razones para el uso de entornos virtualizados? (Elija dos respuestas correctas).
a) Reducir la necesidad de equipos
b) Reducción del riesgo de amenazas
c) Capacidad de aislar las aplicaciones
d) Capacidad de almacenar entornos en dispositivos USB

16) Seleccione las respuestas correctas sobre las políticas recomendadas para las cuentas con contraseña.
a) Hacer que la longitud de la contraseña sea de al menos ocho caracteres y exigir el uso de letras mayúsculas y minúsculas, números y caracteres especiales
b) Exija a los usuarios que cambien las contraseñas cada 60 o 90 días
c) Bloquee las cuentas de los usuarios después de uno o dos intentos fallidos de inicio de sesión
d) Configure el servidor para que no permita a los usuarios utilizar la misma contraseña una y otra vez

17) Al evaluar los activos, ¿cuál de los siguientes factores debe tenerse en cuenta? (Elija tres.)
a) El costo de reposición
b) Su valor para la competencia
c) Su valor para la organización
d) Su valor de recuperación

18) ¿Cuál es el método más común que se utiliza en un programa antivirus?

a) Comprobación de la integridad
b) Escaneo
c) Heurística
d) Métrica

Todos los antivirus realizan un escaneo para verificar si hay vulnerabilidades o amenazas en el sistema, por lo que el escaneo es el método más común.

19) ¿Qué estrategia de gestión de riesgos realiza cuando adquiere un seguro para cubrir los costos de una posible pérdida de datos?
a) Aceptar el riesgo
b) Eliminar el riesgo
c) Mitigar el riesgo
d) Transferir el riesgo

La estrategia es la de transferir el riesgo, pues supongamos que usamos un seguro, entonces los riesgos financieros se transferirán del individuo al asegurador.