Universidad Nacional de Ingeniería

Facultad de Ciencias

Escuela Profesional de Ciencia de la Computación

Seguridad Informática

**Examen de Seguridad Informática**

**SEG Ciclo: 2021-2 Fecha: 30/10/2021**

**Profesor: Sidney Valer Quispe**

1 Pregunta de Teoría (Explicar los nuevos conceptos y justificar su respuesta) 5 puntos

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.

1. La denegación de servicio
2. El malware
3. Ingeniería social
4. Botnets

¿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?

1. DHCP (Dynamic Host Configuration Protocol)
2. NIS (Network Information Service)
3. DNS (Domain Name Service)
4. LDAP (Lightweight Directory Access Protocol)

¿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?

1. Aplicación, sesión, red y física
2. Aplicación, red, sesión y física
3. Presentación, red, transporte y físico
4. Transporte, presentación, red y físico

¿Cómo se puede prevenir una vulnerabilidad de desbordamiento de búfer?

1. Utilizando listas negras que contengan todos los caracteres que puedan ser potencialmente dañinos y no permitiéndolos en la función
2. Instalando parches para corregir las vulnerabilidades de desbordamiento del búfer
3. Programando con C++ en lugar de C porque C++ no es vulnerable a los desbordamientos de búfer como C
4. Utilizando lenguajes de programación fuertemente tipados, implementando la comprobación de límites y entradas, y utilizando funciones de almacenamiento

Un control eficaz contra los ataques de inyección en lenguaje de consulta estructurado (SQL) es

1. Implementar un software antivirus
2. Validar el ingreso de datos del usuario
3. Cifrar las comunicaciones utilizando la seguridad de la capa de transporte (TLS)
4. Desplegar un sistema de prevención de intrusiones

Cinco (5) ejemplos de soluciones exitosas para evitar el robo incluyen

1. Estrictos controles de acceso, sistemas de detección de intrusos, puertos bloqueados, control de claves y control de bag
2. Estrictos controles de acceso, software antiphishing, puertos bloqueados, control de claves y control de bag
3. Identificación y autenticación, sistemas de detección de intrusos, puertos bloqueados, control de claves y comprobación de bag
4. Identificación y autenticación, software antiphishing, puertos bloqueados, control de claves y comprobación de bag

¿Cuál es el papel del auditor?

1. El auditor comprueba la eficacia de los controles implementados por la organización en términos de diseño, aplicación y realiza los cambios necesarios
2. El auditor se asegura que los controles cumplen con el COBIT (Objetivos de Control para TI)
3. El auditor comprueba que los controles cumplen con la norma ISO (Organización Internacional de Normalización) 27001:2005, Anexo A (Sección de Controles)
4. El auditor compara la política declarada con los controles reales existentes

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

1. El responsable local
2. Auditor
3. Propietario de la información
4. Individuo

¿Cuáles son las tres (3) categorías de la informática forense?

1. Investigación de medios, tráfico de red y software
2. Investigación de datos, procesos y sistemas informáticos
3. Investigación de datos, sistemas y personas
4. Investigación de la escena del crimen, las pruebas y los sospechosos

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?

1. Hashing
2. ACLs
3. Atributos de sólo lectura
4. Firewall

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?

1. Disponibilidad
2. Integridad
3. Confidencialidad
4. Negación

¿Cuál es el último paso de un análisis cuantitativo del riesgo?

1. Determinar el valor de los activos.
2. Evaluar la tasa de ocurrencia anualizada.
3. Derivar la expectativa de pérdida anualizada.
4. Realizar un análisis coste/beneficio.

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?

1. Operativo
2. Táctico
3. Resumen
4. Estratégico

¿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?

1. Retorno de la inversión
2. Riesgo
3. Análisis de riesgos
4. Gestión de riesgos

¿Cuáles de las siguientes alternativas son las mejores razones para el uso de entornos virtualizados? (Elija dos respuestas correctas).

1. Reducir la necesidad de equipos
2. Reducción del riesgo de amenazas
3. Capacidad de aislar las aplicaciones
4. Capacidad de almacenar entornos en dispositivos USB

Seleccione las respuestas correctas sobre las políticas recomendadas para las cuentas con contraseña.

1. 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
2. Exija a los usuarios que cambien las contraseñas cada 60 o 90 días
3. Bloquee las cuentas de los usuarios después de uno o dos intentos fallidos de inicio de sesión
4. Configure el servidor para que no permita a los usuarios utilizar la misma contraseña una y otra vez

Al evaluar los activos, ¿cuál de los siguientes factores debe tenerse en cuenta? (Elija tres.)

1. El costo de reposición
2. Su valor para la competencia
3. Su valor para la organización
4. Su valor de recuperación

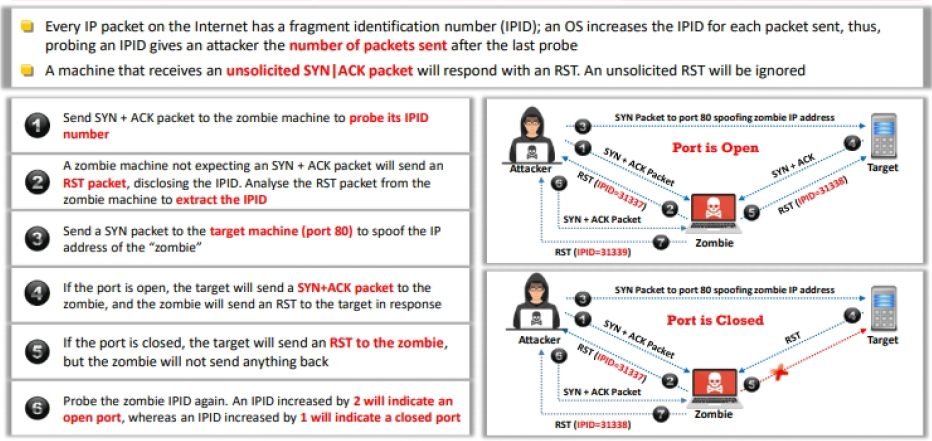
8. Cuál es el método más común que se utiliza en un programa antivirus?

1. Comprobación de la integridad
2. Escaneo
3. Heurística
4. Métrica

¿Qué estrategia de gestión de riesgos realiza cuando adquiere un seguro para cubrir los costos de una posible pérdida de datos?

1. Aceptar el riesgo
2. Eliminar el riesgo
3. Mitigar el riesgo
4. Transferir el riesgo

2.- Realizar una herramienta de escaneo silencioso (idle scanning) con scapy, IDLE es una técnica sigilosa porque oculta la identidad del atacante, la técnica permite realizar escaneos TCP sobre redes IPv4.



* Algoritmo (1 punto)
* Programa (1 punto)
* Explicación del Método (1 punto)
* Evidencias del Resultados (3 puntos)

3.- Realizar una herramienta de trazado de rutas con scapy (traceroute)

Presentar el código y el algoritmo. (2 puntos)

4.- Realizar una el ataque de Hombre en el medio utilizando el ejemplo realizado en clase, el alumno debe implementar un sniffer básico que capture los paquetes para descubrir los datos enviados por la víctima.

* Construir el escenario de prueba (1 punto)
* Explicación del Método (1 punto)
* Evidencias del Resultados (2 puntos)

5.- Realizar un programa para extraer datos sobre el número de infectados por coronavirus en distintas regiones del Perú (Elegir una página de internet que contenga los datos de infectados por coronavirus). (3 puntos)

**Ejemplo de solución de la Pregunta Teóricas**

Bob investiga un incidente de seguridad y descubre que un atacante comenzó con una cuenta de usuario normal, pero consiguió explotar una vulnerabilidad del sistema para conceder a esa cuenta derechos administrativos. ¿Qué tipo de ataque se produjo según el modelo de amenaza STRIDE?

A. Spoofing

B. Repudio

C. Manipulación

D. Elevación de privilegio

Solución:

Subrrayar las palabras desconocida

Bob investiga un incidente de seguridad y descubre que un atacante comenzó con una cuenta de usuario normal, pero consiguió explotar una vulnerabilidad del sistema para conceder a esa cuenta derechos administrativos. ¿Qué tipo de ataque se produjo según el modelo de amenaza STRIDE?

A. Spoofing

B. Repudio

C. Manipulación

D. Elevación de privilegio

Explicar los términos y conceptos desconocidos

**STRIDE** es un modelo de amenazas desarrollado por Praerit Garg y Loren Kohnfelder en Microsof​ para la identificación de [amenazas de seguridad informática](https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica).

**STRIDE** es un modelo de amenazas, utilizado para ayudar a razonar y encontrar amenazas a un sistema. Está utilizado conjuntamente con un modelo del sistema objetivo que puede ser construido en paralelo. Esto incluye un desglose lleno de procesos, base de datos, flujos de datos y fronteras de confianza

**El spoofing** consiste en una serie de técnicas hacking, por lo general, con intenciones maliciosas, creadas para suplantar la identidad de entidades o personas en la red, con el objetivo de obtener información privada o para conseguir acceder a páginas con una credencial falsa.

Respuesta de la pregunta

D. En un ataque de elevación de privilegios, el atacante transforma una cuenta de usuario limitada en una cuenta con mayores privilegios, poderes y/o acceso al sistema. Los ataques de suplantación(Spoofing) de identidad falsifican una identidad, mientras que los ataques de repudio intentan negar la responsabilidad de una acción. Los ataques de manipulación intentan violar la integridad de la información o de los recursos.