Universidad Nacional de Ingeniería

Facultad de Ciencias

Escuela Profesional de Ciencia de la Computación

Seguridad Informática

**Examen de Seguridad Informática**

**SEG Ciclo: 2021-I Fecha:05/06/2021**

**Profesor: Sidney Valer Quispe**

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

Usted como especialista experto de seguridad informática de una empresa tiene la responsabilidad de asesorar en materia de seguridad al departamento de tecnología. Su principal preocupación para capacitar a los empleados de la empresa en materia de concienciación de seguridad es defenderse de.

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

Explicación de términos desconocidos:

**La denegación de servicio**, cuando un sistema de computadoras o red causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

**El malware** es un término general para referirse a cualquier tipo de “malicious software” (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento.

La definición de **botnets** es que es un grupo de PC infectados y controlados por un atacante de forma remota.

La **ingeniería social** es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información​ que les permitan realizar daños a la persona u organismo comprometidos

Cuando hablando de materia de concienciación de seguridad nos referimos al aspecto cognitivo de entender lo que conlleva la ciberseguridad en todos sus aspectos por lo tanto

¿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)

Explicación de términos desconocidos:

¿Qué afirmación es VERDADERA en relación con la seguridad del protocolo de Internet (IP)V4 e IPV6?

1. IPV6 es menos seguro que IPV4. IPV6 permite que cada nodo tenga su propia dirección IP. IPV4 permite blindar las direcciones privadas detrás de las direcciones públicas
2. IPV6 es menos seguro que IPV4. Aunque sigue existiendo un organismo centralizador, ahora es internacional y las organizaciones criminales pueden ahora obtener direcciones IP.
3. IPV6 es más seguro que IPV4. IPV6 obliga a utilizar el protocolo de seguridad de Internet (IPSec)
4. IPV6 es más seguro que IPV4. Sólo las empresas que han sido aprobadas por el gobierno pueden utilizarlo

Explicación de términos desconocidos:

**“IPV6 es más seguro que IPV4”.** Los orígenes de este mito se remontan a la primera especificación de IPv6. En aquel momento, el soporte IPsec era obligatorio para IPv6, se esperaba un amplio despliegue de IPv6+IPsec a corto plazo y se pensaba que los proveedores no se molestarían en añadir soporte IPsec a sus implementaciones IPv4. Sin embargo, estas previsiones no se cumplieron: casi todas las implementaciones más populares de IPv4 incorporaron soporte para IPsec, y el conjunto IPv4+IPsec se desplegó mucho antes que cualquier despliegue significativo de IPv6 (por no citar el binomio IPv6+IPsec).

La computación en nube implica el acceso a software y datos a través de Internet en servidores gestionados por un proveedor externo. Los acuerdos de computación en nube aumentan la disponibilidad, ofrecen una mayor escalabilidad y

1. Aumentan la confidencialidad
2. Aumentan las posibilidades de ataque
3. Aumentar la integridad
4. Eliminar la necesidad de cifrar los datos

¿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

Explicación de términos desconocidos:

1. **Capa de aplicación**
2. **Capa de presentación**
3. **Capa de sesión**
4. **Capa de transporte**
5. **Capa de control de red**
6. **Capa de enlace de datos**
7. **Capa física**

La d no puede ser porque la capa de presentación esta más próxima al usuario que la capa de transporte. Pasa lo mismo en la c ya que la capa de transporte esta más cerca al usuario final que la de red. Por último en la b la de red está más alejada del usuario final que la de sesión quedando nos como respuesta la a, a**plicación, sesión, red y física.**

¿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

Explicación de términos desconocidos:

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

1. Implementar un software antivirus
2. Validar la entrada 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

¿Cuál de las siguientes opciones describe MEJOR lo que debería ser el cumplimiento, de acuerdo con

1. La ley, las reglas de la organización y las normas del sector
2. Las directrices, las especificaciones y la legislación
3. Normas, reglamentos y directrices
4. Las normas pertinentes de la Organización Internacional de Normalización (ISO)

La persona con la mayor responsabilidad del cumplimiento, que se establece en los niveles de clasificación y los controles de acceso para cada activo de información sensible es el

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

Un método de auditoría utilizado para realizar automáticamente el control de las evaluaciones de riesgo con mayor frecuencia se conoce como

1. Certificación
2. Control continuo
3. Acreditación
4. Revisión periódica

La **certificación** es formalización de la técnica de investigación, cuando, por su importancia, resulta conveniente que las afirmaciones recibidas deban quedar escritas (declaraciones) y en algunas ocasiones certificadas por alguna autoridad (certificaciones).

¿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

Explicación de términos desconocidos:

La **confidencialidad** se refiere a los esfuerzos de una organización para mantener sus datos privados o secretos. En la práctica, se trata de controlar el acceso a los datos para evitar su divulgación no autorizada.

La **integridad** se refiere a la entereza de algo. En seguridad informática, la integridad consiste en garantizar que los datos no hayan sido manipulados y, por lo tanto, sean confiables.

La **accesibilidad** significa que las redes, los sistemas y las aplicaciones están en su pleno funcionamiento. Ello garantiza que los usuarios autorizados tengan acceso oportuno y fiable a los recursos cuando los necesiten.

La **denegación** es que el rendimiento de un sistema, sitio web, aplicación basada en la web o servicio basado en la web, se degrada de forma intencional y maliciosa. Con ello, el sistema se vuelve completamente inalcanzable. No es un de los tres principios.

Respecto al problema, entre los tres principios, el de **disponibilidad(accesibilidad)** se está violando al haber un bombardeo de paquetes porque impide el flujo en la red.

¿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.

Explicación de términos desconocidos:

El análisis cuantitativo de riesgos es una forma de estimar numéricamente la probabilidad de que un proyecto cumpla con sus objetivos de costo y tiempo.

En la gestión de riesgos uno de los primeros pasos a realizar es la realización de **análisis de coste y beneficio.** Esta no está dentro delanálisis cuantitativo del riesgo es parte de la gestión de riesgos.

Se puede **determinar el valor de los activos** con el valor de compra del activo y restarle el valor de rescate (precio que se podría obtener una vez que llegue al fin de su vida útil**).**

La **tasa anualizada de ocurrencia** es una estimación de la frecuencia con la que una amenaza tendría éxito en explotando una vulnerabilidad. Mientras tanto La **expectativa de pérdida** **anualizada** es el producto de la **tasa anual de ocurrencia** (ARO) y la expectativa de pérdida única.

Nosotros buscamos al final de un análisis cuantitativo del riesgo **expectativa de pérdida** **anualizada.**

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

Explicación de términos desconocidos:

El **resumen** no es plan de desarrollo.

Una **planificación estratégica** describe su misión, visión y objetivos de alto nivel para los próximos tres a cinco años. También tiene en cuenta cómo va a medir esos objetivos y los principales proyectos que llevará a cabo para alcanzarlos.

La **planificación estratégica** se desdobla para toda la organización, la **planificación táctica** tiene una participación más limitada, a nivel departamental, involucrando a veces sólo un proceso de punta a punta. La **planificación táctica** es el responsable de crear metas y condiciones para que las acciones establecidas en la planificación estratégica sean alcanzadas.

Una **planificación operativa** (también conocido como plan de trabajo) es un resumen de lo que su departamento se enfocará en el futuro cercano, generalmente el próximo año.

En pocas palabras, su **plan estratégico** comparte su visión para el futuro, mientras que su **planificación operativ**a establece cómo llegará allí diariamente o semanalmente.

2.- Realizar una herramienta de escaneo de puerto con scapy, la herramienta debe utilizar las siguientes técnicas de exploración de puertos TCP.

* TCP SYN Scan
* TCP FIN Scan
* TCP Xmas Tree Scan
* TCP Null Scan
* UDP Scan

Presentar el código y el algoritmo de cada técnica.

Revisar:

<https://www.seguridadyfirewall.cl/2017/12/tecnicas-de-exploracion-tcp-port_21.html>

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

Presentar el código y el algoritmo.

4.- Realizar una herramienta que capture los datos de autos que se ofrecen en una página que ofrece en venta autos usados, según su marca y tipo (Mecánica, Automática)

**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.