MATERIALES DOCENTES DE LA ASIGNATURA INTRODUCCIÓN A LA CIBERSEGURIDAD

BLOQUE 5: EJEMPLOS DE PRUEBAS DE EVALUACIÓN

CURSO ACADÉMICO 2022-2023

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

Universidad Rey Juan Carlos

Marta Beltrán Pardo

5. EJEMPLOS DE PRUEBAS DE EVALUACIÓN

Prueba final, Introducción a la Ciberseguridad
PRIMERA CONVOCATORIA, DICIEMBRE 2018

NOMBRE Y APELLIDOS:

DNI:

- Dispones de 90 minutos para la realización de esta prueba.
- En cada pregunta se indica la puntuación que le corresponde.
- No se permite la utilización de ningún material (apuntes, etc.), encima de la mesa sólo puedes tener el bolígrafo que utilices para contestar.
- Puedes contestar a las preguntas con la extensión y orden que tú decidas.

1. ¿Qué es la criptografía? ¿Y la esteganografía? Señala las semejanzas que hay entre ellas así como las diferencias. **(1.5 puntos)**
2. ¿Qué es el repertorio de instrucciones de un computador? ¿Qué tres tipos de instrucciones debe incluir? ¿Debe un programador conocer estos repertorios de instrucciones a bajo nivel? ¿Y un profesional de la ciberseguridad? **(1 punto)**
3. ¿Qué tres aspectos debe garantizar la Seguridad Informática? Pon un ejemplo de amenaza actual para cada uno de ellos. **(1.5 puntos)**
4. ¿En qué consiste el proceso de autenticación de un usuario por parte de un sistema operativo? ¿Qué alternativas tenemos para construir estos procesos de autenticación? **(1 punto)**
5. ¿Qué es una política de seguridad y para qué sirve? Explica por qué son necesarias estas políticas y qué partes las componen. **(1.5 puntos)**
6. ¿Qué son las cookies y para qué se usan? ¿Qué ventajas e inconvenientes tiene su uso desde el punto de vista de la seguridad? **(1 punto)**
7. Durante la ejecución de un patrón de ataque ¿qué son las técnicas de footprinting y fingerprinting? ¿para qué sirven? ¿en qué se diferencian? Menciona las más importantes de ambos tipos que conozcas. **(1.5 puntos)**
8. ¿Qué es el modelo STRIDE, cómo se utiliza y para qué sirve? **(1 punto)**

Prueba final, Introducción a la Ciberseguridad
SEGUNDA CONVOCATORIA, JUNIO 2019

NOMBRE Y APELLIDOS:

DNI:

- Dispones de 90 minutos para la realización de esta prueba.
- En cada pregunta se indica la puntuación que le corresponde.
- No se permite la utilización de ningún material (apuntes, etc.), encima de la mesa sólo puedes tener el bolígrafo que utilices para contestar.
- Puedes contestar a las preguntas con la extensión y orden que tú decidas.

1. Define los conceptos de riesgo, amenaza y vulnerabilidad y señala las relaciones que hay entre ellos. **(1.5 puntos)**
2. ¿Qué es el CVE? ¿Y el CVE-ID de una vulnerabilidad? ¿Y el CVSS? ¿Para qué sirve todo esto, qué utilidad tiene para la comunidad? **(1 punto)**
3. ¿Qué diferencia hay entre el control de acceso MAC y el DAC en un sistema operativo? ¿En qué consiste el RBAC en este mismo contexto? **(1 punto)**
4. Cuando se trata de encontrar vulnerabilidades en un software ¿qué tipos de análisis de código conoces y en qué se diferencian? **(1 punto)**
5. ¿Qué es un Insider Threat? ¿Cómo pretende lidiar con esta amenaza un ITP (Insider Threat Program)? **(1.5 puntos)**
6. ¿Qué nombres, identificadores o direcciones se utilizan en TCP/IP y a qué nivel está cada uno de ellos? ¿Qué problemas de seguridad puede implicar la traducción de unos a otros? **(1 punto)**
7. ¿Qué tipos de malware conoces? ¿Qué características distinguen a cada uno de estos tipos? **(1.5 puntos)**
8. ¿Por qué los atacantes o adversarios suelen buscar el anonimato? ¿Qué tipo de técnicas utilizan y cómo funcionan? **(1.5 puntos)**

Prueba final, Introducción a la Ciberseguridad
PRIMERA CONVOCATORIA, ENERO 2020

NOMBRE Y APELLIDOS:

DNI:

- Dispones de 90 minutos para la realización de esta prueba.
- En cada pregunta se indica la puntuación que le corresponde.
- No se permite la utilización de ningún material (apuntes, etc.), encima de la mesa sólo puedes tener el bolígrafo que utilices para contestar.
- Puedes contestar a las preguntas con la extensión y orden que tú decidas.

1. ¿Por qué el cifrado y la fortificación ya no pueden ser, exclusivamente, las bases de la ciberseguridad? ¿En qué tres principios se basa esta ciberseguridad en la actualidad? Explica qué implica cada uno de ellos. **(1.5 puntos)**
2. ¿Qué es el CVE? ¿Y el CVE-ID de una vulnerabilidad? ¿Y el CVSS? ¿Para qué sirve todo esto, qué utilidad tiene para la comunidad? **(1 punto)**
3. Intenta explicar los conceptos de protección y seguridad, diferenciándolos claramente y relacionándolos con los sistemas operativos. ¿Qué tipo de recursos tiene que proteger el sistema operativo? ¿Qué cuatro tipos de separación se suelen emplear en los sistemas operativos actuales para garantizar la protección? **(1 punto)**
4. ¿Qué normas son básicas para la construcción y mantenimiento de una contraseña segura? Justifica cada una de ellas. **(1 punto)**
5. ¿Cuáles son las causas más habituales de los bugs o vulnerabilidades de código? Menciona algunas mejores prácticas que podrían ayudar a reducir su número. **(1 punto)**
6. ¿Qué es una política de seguridad y para qué sirve? Explica qué partes la componen y menciona alguna típica que suelan tener definida casi todas las organizaciones. **(1.5 puntos)**
7. ¿Qué significa el acrónimo APT? ¿Qué tipo de amenaza es y qué la caracteriza? ¿En qué tipo de contextos se suele observar hoy en día? ¿Existen contramedidas o mitigaciones específicas para proteger a una organización contra ellas? **(1.5 puntos)**
8. ¿Qué es STRIDE y para qué sirve? Explica este modelo brevemente y justifica su importancia. **(1.5 puntos)**

Prueba final, Introducción a la Ciberseguridad
PRIMERA CONVOCATORIA, ENERO 2022

NOMBRE Y APELLIDOS:

DNI:

- Dispones de 90 minutos para la realización de esta prueba.
- En cada pregunta se indica la puntuación que le corresponde.
- No se permite la utilización de ningún material (apuntes, etc.).
- Encima de la mesa sólo puedes tener el bolígrafo que utilices para contestar.
- Puedes contestar a las preguntas con la extensión y orden que tú decidas.

1. ¿Qué es la criptografía? ¿Qué pilares de la seguridad nos puede ayudar a proteger y cómo? Usa ejemplos para contestar a esta segunda pregunta. **(1.5 puntos)**
2. Explica por qué los conceptos de riesgo, amenaza y vulnerabilidad están relacionados, pero son diferentes. Pon un ejemplo de cada uno de ellos (uno de riesgo, uno de amenaza y uno de vulnerabilidad) y aprovecha el ejemplo para mostrar esta relación. **(1.5 puntos)**
3. Explica los conceptos de protección y seguridad, diferenciándolos claramente y relacionándolos con los sistemas operativos. ¿Todos los sistemas operativos garantizan protección? ¿Cómo? ¿Y seguridad? ¿Cómo? Razona tu respuesta. **(1.5 puntos)**
4. ¿En qué base de datos se publican las vulnerabilidades de software que se van descubriendo? Explica cómo funciona esta base de datos, para qué sirve y qué proceso se sigue para publicar en ella una vulnerabilidad. ¿Te parece bien el funcionamiento de esta base de datos, o hay alguna crítica que se le pueda hacer, cómo podríamos mejorarla? **(1.5 puntos)**
5. ¿Qué es el phishing y qué pretende? ¿Qué tipos específicos de phishing conoces y por qué sus tasas de éxito son tan altas? ¿Cómo se puede mitigar este tipo de amenaza? **(1 punto)**
6. ¿Qué es STRIDE? Explica este modelo brevemente. ¿Cómo se usa y para qué sirve? **(1.5 puntos)**
7. Explica brevemente qué es el malware, qué tipos de malware hay y qué mecanismos distinguen a unos de otros. ¿Cuál crees que es el más preocupante en la actualidad y por qué? **(1.5 puntos)**

Prueba final, Introducción a la Ciberseguridad
CONVOCATORIA EXTRAORDINARIA, JUNIO 2022

NOMBRE Y APELLIDOS:

DNI:

- Dispones de 90 minutos para la realización de esta prueba.
- En cada pregunta se indica la puntuación que le corresponde.
- No se permite la utilización de ningún material (apuntes, etc.).
- Encima de la mesa sólo puedes tener el bolígrafo que utilices para contestar.
- Puedes contestar a las preguntas con la extensión y orden que tú decidas.

1. Explica las características que un buen criptosistema debería cumplir según Shannon y justifica cada una de ellas con un ejemplo de aplicación de la criptografía en el campo de la ciberseguridad. **(1.5 puntos)**
2. Explica los conceptos de evento de seguridad, ataque e incidente; haciendo hincapié en las diferencias entre ellos y poniendo un ejemplo de cada uno de ellos. **(1.5 puntos)**
3. ¿Qué es un sistema operativo de confianza, en qué se diferencia de uno que no lo sea y para qué sirve? ¿Conoces alguno? ¿Con qué nivel de seguridad? ¿Cómo se mide este nivel? **(1.5 puntos)**
4. Explica los conceptos de zero-day, tiempo de reacción, parche de software y exploit. Relaciónalos y pon un ejemplo (imaginario) para hacerlo. **(1.5 puntos)**
5. ¿Qué es un Plan Director de Seguridad y cómo se define? ¿Qué aspectos crees que son críticos para definir un plan de este tipo que sea útil? ¿Qué relación tiene con la gestión del factor humano? **(1.5 puntos)**
6. ¿Qué significa el acrónimo APT? ¿Qué tipo de amenaza es y qué la caracteriza? ¿Qué relación tiene con el malware? **(1 punto)**
7. ¿Por qué los atacantes suelen buscar el anonimato? ¿Qué tipo de técnicas utilizan y cómo funcionan? ¿Cuáles son sus ventajas e inconvenientes desde el punto de vista del atacante? **(1.5 puntos)**