Tarea online HE01.

Título de la tarea: Pautas de seguridad informática

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Contenidos

1.- Conceptos generales en hacking ético.
- 1.1.- Diferencias entre actores/actividades éticas o criminales.
- 1.2.- Seguridad de la información vs seguridad informática.
- 1.3.- Principios de la seguridad de la información.

2.- Concepto de Riesgo y Vulnerabilidad.
- 2.1.- Valoración de vulnerabilidades.
- 2.2.- Clasificación de vulnerabilidades.

3.- Auditorías de hacking ético.
- 3.1.- Tipos de auditoría dependiendo del enfoque.
- 3.2.- Tipos de auditoría dependiendo del origen.
- 3.3.- Tipos de auditoría dependiendo de la información proporcionada.
- 3.4.- Fases de una auditoría.
  - 3.4.1.- Pre-engagement o toma de requisitos.
  - 3.4.2.- Ejecución de las pruebas.
  - 3.4.3.- Seguimiento de las pruebas.
  - 3.4.4.- Reporting o generación de informes.
  - 3.4.5.- Cierre de auditoría.

4.- Herramientas de seguridad y hacking ético.
- 4.1.- Herramientas de Descubrimiento y Reconocimiento.
- 4.2.- Herramientas de Escaneo y Monitorización.
- 4.3.- Herramientas de Explotación.
- 4.4.- Herramientas de Postexplotación.

Resultados de aprendizaje

RA1. Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.

1.- Descripción de la tarea.

Caso práctico

Una vez han completado la creación del nuevo departamento de "Seguridad Ofensiva" y Juan, junto con su equipo han finalizado las sesiones de formación. Teresa les reúne para asignarles su primer cometido.

Direct Media (Dominio público)

Teresa les comenta que el primer cometido del equipo es diseñar un plan de auditoría para este primer trimestre. Dado que es la primera vez que se enfrentan a un reto de estas características ha acordado con la dirección que este primer trimestre les realizará la auditoría una empresa externa. Además, el presupuesto asignado para este trimestre sólo permite que se realicen un máximo de 5 auditorías

El equipo de Juan tiene que diseñar el tipo de auditorías que se realizará teniendo en cuenta las siguientes premisas:

- Disponen de un total de 20 activos expuestos a internet entre servidores web, servidores de correo, acceso VPN.
- De estos 20 activos, 3 de ellos se consideran críticos para el negocio
- Además, también les interesa realizar una primera revisión de la red interna.

¿Qué te pedimos que hagas?

- **Apartado 1: Diseñar el plan de auditoría**

  Teniendo en cuenta las premisas y restricciones indicadas por teresa diseñar el plan de auditoría. Como mínimo has de plantear y explicar las siguientes cuestiones y razonar correctamente tu elección:

  - Indicar que tipo de auditorías realizarías y sobre los activos, necesitas elaborar tu respuesta con las siguientes premisas:
    - Justificar la elección de cada auditoría elegida.
    - Justificar los activos incluídos en cada auditoría.
    - Indicar en cada caso el tipo de auditoría dependiendo del enfoque, orígen e información proporcionada y justifica cada caso

- Indica el objetivo que quieres conseguir con la elección de cada tipo de auditoría.

- **Apartado 2: Organiza las fases de la auditoría**

Una vez has planteado las auditorías que realizarías, es necesario que indiques para cada una de ellas un calendario (o timeline) en el que se refleje los hitos de cada una de las fases con estimaciones de tiempo:

- Utiliza un calendario o línea temporal para indicar cuándo se realizaría cada fase y el tiempo estimado.
- Indica los objetivos a cumplir en cada fase.
- Justifica para cada auditoría si se contemplan reuniones de seguimiento o no, en caso afirmativo cada cuánto tiempo.

- **Apartado 3: Presentación y valoración de vulnerabilidades.**

En este caso nos ponemos en el lado de los auditores y tenemos que analizar siguientes vulnerabilidades que se han localizado durante las pruebas. Para cada una de ellas hay que completar la siguiente descripción.

- Valoración de la vulnerabilidad especificando los grupos de métricas base y temporal. Además, indica el vector CVSS resultante, realizar capturas de pantalla de los valores indicados.
- Es muy importante justificar vuestra elección en los puntos del formulario CVSS.
- Justificar si es una vulnerabilidad que afecta al servidor o a los clientes.

- **Las vulnerabilidades localizadas son las siguientes.**

  - Una vulnerabilidad en el sistema de correo de la compañía que permite tomar el control del servidor y acceder a los mensajes de correo de cualquier usuario, también puedes enviar correos electrónico suplantando la identidad de los usuarios. El servidor de correo se encuentra expuesto en internet. La vulnerabilidad presenta tanto un exploit público accesible desde exploit-db como un parche propuesto por el fabricante.
  - Una vulnerabilidad de inyección SQL en la que se pueden consultar datos de otras Bases de Datos como la Base de Datos de Contabilidad. El servidor web está expuesto en internet, pero se requiere de un usuario para el acceso a la funcionalidad vulnerable. No es una vulnerabilidad conocida, el auditor la localizó en tiempo de auditoría.
  - Una vulnerabilidad de ejecución remota de código en un servidor FTP en la red interna de la organización. El servicio FTP se estaba ejecutando con privilegios del sistema (puede realizar cualquier acción en el sistema). Además, el acceso al servidor permite acceder a una subred de administración que no se encuentra accesible desde la red LAN de usuarios. Existe un parche público para corregir la vulnerabilidad. No hay exploit público, pero sí una prueba de concepto que el auditor ha tenido que modificar par poder explotar de manera correcta la vulnerabilidad.

NOTA IMPORTANTE

Para los apartados en los que se solicita realizar una captura de pantalla hay que tener en cuenta que las capturas realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM
- Conexión a Internet para consultar ejemplos de la Unidad 1.
- Sistemas Operativos con herramientas ofimáticas.
- Navegador web.
- Software para comprimir los archivos de la tarea.

Material ajunto:

- Documentación sobre CVSS 3.1.

Recomendaciones

- Antes de abordar la tarea:
  - lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_HE01_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la primera unidad del MP de HE**, debería nombrar esta tarea como...

sanchez_manas_begona_HE01_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación RA1

- a. Se ha definido la terminología esencial del hacking ético.
- b. Se han identificado los conceptos éticos y legales frente al ciberdelito.
- c. Se han identificado los elementos esenciales de seguridad: confidencialidad, integridad y disponibilidad.
- d. Se ha definido el alcance y condiciones de un test de intrusión.
- e. Se han identificado las fases de un ataque seguidas por un atacante.
- f. Se han analizado y definido los tipos vulnerabilidades.
- g. Se han analizado y definido los tipos de ataque.
- h. Se han determinado y caracterizado las diferentes vulnerabilidades existentes.
- i. Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Criterio 1: Indica y justifica de manera correcta la elección de las distintas auditorías elegidas en su diseño del plan de auditorías. Al menos cuatro auditorías.	1 punto (obligatorio)
Apartado 1: Criterio 2: Indica y justifica de manera correcta los activos a incluir en el alcance de cada auditoría elegida. Al menos cuatro auditorías.	1 punto (obligatorio)
Apartado 1: Criterio 3: Indica y justifica de manera correcta el tipo de auditoría elegida según el orígen de pruebas, información proporcionada y enfoque elegidos para cada una de las auditorías del plan. Al menos cuatro auditorías.	1 punto (obligatorio)
Apartado 1: Criterio 4: Indica y justifica de manera correcta el objetivo que se pretende cubrir en cada una de las auditorías recogidas del plan. Al menos cuatro auditorías.	1 punto (obligatorio)

Apartado 2: Criterio 1: Proporciona un calendario de actividad con las fases de auditoría de cada una de las auditorías elegidas con un tiempo estimado acorde al número de activos y tipología de auditoría. Al menos cuatro auditorías.	1 punto (obligatorio)
Apartado 2: Criterio 2: Indica de manera correcta los hitos a cumplir en cada fase de las auditorías elegidas. Al menos cuatro auditorías.	1 punto (obligatorio)
Apartado 2: Criterio 3: Indica y justifica si en alguna de las auditorías elegidas se contemplan reuniones de seguimiento y en un tiempo prudencial. Al menos cuatro auditorías.	1 punto (obligatorio)
Apartado 3: Criterio 1: Realiza una valoración correcta de la primera vulnerabilidad indicando el vector CVSS resultante y la puntuación resultante.	0,34 puntos (obligatorio)
Apartado 3: Criterio 2: Realiza una valoración correcta de la segunda vulnerabilidad indicando el vector CVSS resultante y la puntuación resultante.	0,33 puntos (obligatorio)
Apartado 3: Criterio 3: Realiza una valoración correcta de la tercera vulnerabilidad indicando el vector CVSS resultante y la puntuación resultante.	0,33 puntos (obligatorio)
Apartado 3: Criterio 4: Justifica de manera precisa la elección cada uno de los valores de las métricas utilizadas en la calculadora CVSS para valorar la primera vulnerabilidad.	0,34 puntos (obligatorio)
Apartado 3: Criterio 5: Justifica de manera precisa la elección cada uno de los valores de las métricas utilizadas en la calculadora CVSS para valorar la segunda vulnerabilidad.	0,33 puntos (obligatorio)
Apartado 3: Criterio 6: Justifica de manera precisa la elección cada uno de los valores de las métricas utilizadas en la calculadora CVSS para valorar la tercera vulnerabilidad.	0,33 puntos (obligatorio)
Apartado 3: Criterio 7: Indica y justifica de manera correcta si las tres vulnerabilidades descritas afecta al servidor o al cliente	1 punto (obligatorio)
Redacción clara y correcta, sin errores ortográficos	**Se resta 0,1 puntos por cada error ortográfico o expresiones incorrectas.**

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.