MUIInf
Máster Oficial Universitario en
Ingeniería Informática
muiinf.webs.upv.es

UNIVERSITAT POLITÈCNICA DE VALÈNCIA
etsinf

Trabajos de Asignatura

Ciberseguridad 2023-2024

Introducción

Como podrás comprobar, los enunciados de los trabajo son “intencionadamente” muy poco concretos. La idea es que seas capaz de trabajar con peticiones ambiguas e incompletas. Y que seas tú mismo el que diseñe los informes que tendrás que presentar a los “jefes”. En el mundo de la empresa los directivos saben menos que los técnicos, y por tanto, no son capaces de enunciar las tareas técnicas de forma precisa. Es tarea del especialista ser capaz de analizar, comprender o incluso cuestionar los objetivos que se piden.

Por tanto, no quiero que los enunciados de los trabajos se conviertan en formularios donde solo quede por rellenar los huecos. Tampoco quiero que los trabajos sean una secuencia de acciones preestablecidas donde sabemos a priori que todo va a funcionar y que todo es factible. Si una solución no funciona, pues se busca otra y se continua.

En la última sección de este documento se dan varios consejos sobre la estructura y estilo de las memorias.

Trabajo 1: Actualidad en ciberseguridad

La ciberseguridad es un sector en constante evolución. Es seguro que a lo largo del curso sucederán hechos relevante que deberemos conocer, tanto ciber-incidentes, como nuevas soluciones de seguridad, legislación, etc.

Uno de los problemas a los que se enfrentan los expertos en seguridad es la recopilación y organización de la gran cantidad de información generada.

El objetivo del trabajo consiste en recopilar aquellos hechos que consideres más significativos y realices un pequeño informe sobre cada uno de ellos. El informe contendrá al menos CINCO (5) “security issues”.

Nota: Puesto que existen multitud de servicios de recopilación de información de seguridad, el trabajo no se debe limitar a copiar los incidentes, sino que se debe justificar convenientemente los motivos por lo que se han seleccionado y el impacto que pueden tener.

Contenido de la memoria

Cada uno de los cinco incidentes debe estar en una sección. Donde se describirá el tipo de fallo, el CVE asignado y el *score* CVSS, en caso de no disponer del CVSS debes tratar de calcularlo, también se tiene que presentar el impacto que el fallo ha tenido en la sociedad (a quién afecta, y cómo). Finalmente, comentar las posible medidas de prevención o mitigación que se deberían utilizar.

Puesto que cada fallo o incidente puede ser muy distinto, el contenido se adaptará a las características concretas de cada uno.

Trabajo 2: Cifrado de la información

Un mecanismo de protección contra ataques de robo de información consiste en el cifrado de los datos. Este cifrado se puede realizar cuando la información está en transito entre dos sistemas (el más conocido es TLS) o cuando está almacenada en un medio permanente.

En este trabajo se abordará en cifrado de mail y de los datos almacenados en discos.

El trabajo consistirá en:

1. Buscar información sobre las aplicaciones de cifrado de ficheros en Linux. Se deben utilizar varias y ver las ventajas e inconvenientes.
2. Crearse una clave PGP y compartirla en un servidor público de claves PGP.
3. Realizar una instalación de un sistema Linux sobre una partición cifrada con LUKS.

Tienes que demostrar que eres capaz de cifrar ficheros ficheros para uso personal, enviar y recibir información cifrada con otros compañeros, y trabajar con un ordenador que tenga todos los datos cifrados.

La memoria la tienes que subir a Poliformat (sin cifrar) y enviármela por email cifrada de tal forma que solo yo y los autores del informe puedan leerla.

Contenido de la memoria

Piensa lo que se te pide y organiza la memoria de la forma más coherente que puedas. Fíjate que puedes explicar el gnupg en una sección y en otra usarlo para crear la clave PGP. Lo cual va a hacer que la estructura del documento sea un poco “rara”.

Piensa cómo te gustaría que te lo contaran y estructuraran los contenidos.

No quiero que sea un *colage* de recetas o de información sacada de la wikipedia. La mayor parte del trabajo consiste en comprender los conceptos básicos de criptografía, qué herramientas existen, las particularidades de usos de cada una, y utilizar dos soluciones de cifrado, por tanto la organización de toda esa información es súper importante.

Trabajo 3: Contribuir a la Wikipedia

[**Este trabajo es opcional. Y sirve para subir nota.**]

Seguramente, hasta ahora solo has sido consumidor de información (libros, apuntes, presentaciones, manuales, Wikipedia, etc.), pero al llegar a los últimos años de la carrera, ya es momento de empezar a generar y publicar información de calidad.

La Wikipedia es una magnífica fuente de información. En ella se encuentran desde temas muy generales hasta cuestiones específicas de una rama del conocimiento; y desde artículos amplios, hasta breves reseñas con poco más que una definición de diccionario.

Este trabajo consiste en identificar alguna entrada de la Wikipedia relacionada con la ciberseguridad y ampliarla con los conocimientos que hayas adquirido. Para ellos será necesario que te documentes bien para poder estructurar y resumir la información que vas a publicar.

La aportación debe seguir los siguientes criterios:

- La entrada que elijas no debe existir en otro idioma. No sirve hace runa traducción.
- Puedes utilizar una entrada que ya exista añadiendo nueva información.
- Deben seguir el estilo de redacción que define la Wikipedia.
- Recuerda referenciar todas las fuentes que utilices.

Estilo de las memorias

1. Toda memoria debe tener una portada con el título, los autores y alguna referencia al grado.

   Cuando preparéis un trabajo en la empresa deberéis indicar claramente el título, el departamento al que pertenece y todas las referencias necesarias para identificar el contexto del trabajo.

2. Debe tener un índice con capítulos, secciones y subsecciones.

   Poner un índice de tablas o figuras no suele ser necesario. Dependiendo de la audiencia, poner un glosario de términos y siglas puede ser interesante.

3. El primer capítulo debe contener un resumen del contenido del documento (lo que sería un “resumen ejecutivo”). Este resumen debe responder a las siguiente preguntas:

   1. ¿Por qué se ha realizado el informe? ¿Qué lo ha motivado?
   2. ¿Qué encontrará el lector? ¿Qué se ha resuelto?
   3. Cómo está estructurado.

      La idea es que al acabar la introducción el lector debe saber si lo puede leer y si le va a interesar. En el caso de estas memorias, el primer capítulo será muy breve, pero es bueno acostumbrarse a pensar de esta forma.

4. Añadir una sección al final que sean las conclusiones, donde se resume lo más importante del trabajo. Recuerda que las conclusiones no debe contener material nuevo solo resumir lo que ya se ha explicado y demostrado. Por tanto en las conclusiones no deben haber citas a trabajos externos. Al igual que con el capítulo de introducción, en este caso, las conclusiones no tienen que ser muy extensas.

5. Es necesario referenciar correctamente todas las citas. También hay que mencionar la autoría o referenciar correctamente las imágenes.

   Es bueno que practiquéis con la bibliografía porque en el TFM suele ser un aspecto donde el tribunal se fija mucho.

6. Se debe usar la fuente **`Courier`** (o una de ancho ancho fijo, o typewriter) para el código o capturas de pantalla. Nunca se deben usar fuentes proporcionales en código porque puede estropear la indentación.

7. La capturas de pantalla deben ser visualmente correctas:

   1. Se tienen que poder leer.
   2. No se deben sobre-escalar, de forma que se vean pixeladas (repite la toma si es necesario).
   3. Se debe guardar las proporciones entre imágenes con contenidos similares.

Por ejemplo, si una ventana de dialogo es pequeña, entonces no hay que escalarla para que ocupe lo mismo que otra captura de la aplicación completa.

8. Todas las imágenes deben tener un "*caption*" o leyenda. Y mejor si la imágenes aparecen referenciadas o comentadas en el texto.