Auditoría y Legislación Informática

Resuelve y construye tu CTF

UNIVERSIDAD DE EXTREMADURA

Auditoría y Legislación Informática

Resuelve y construye tu CTF

Índice

1. Introducción

Esta práctica se centra en conocer conceptos básicos, aunque bastantes desconocidos, de la informática forense como son la esteganografía, la criptografía y las técnicas de OSINT (Open Source Intelligence en español Inteligencia de Fuentes Abiertas).

Se utilizará la metodología activa de Aprendizaje Basado en Retos cuyo enfoque pedagógico involucra activamente a los estudiantes en una situación de problema real y relacionada con su entorno, tomando éste un papel trascendental en la búsqueda de la solución. Para ello se utilizará el tipo de reto denominado Capture The Flag (en español, Captura la Bandera) que consiste en resolver un desafío informático que pone a prueba nuestros conocimientos.

2. Objetivos

Los objetivos de la prácticas son los siguientes:

- Conocer de manera básica y práctica los conceptos de esteganografía, criptografía y técnicas de OSINT.
- Conseguir resolver el reto propuesto por los profesores de la asignatura mediante la adquisición de los conceptos anteriormente expuestos.
- Ser capaz de seguir un procedimiento para construir un reto similar al presentando por los profesores de la asignatura.
- Generar una documentación técnica que recoja el procedimiento seguido por los estudiantes para construir su propio reto y resolver uno propuesto por otro compañero/a de la asignatura.

3. Materiales

Para la realización de esta práctica se entregan a través del aula virtual de la asignatura los siguientes materiales:

- Una imagen denominada "*pista*" cuyo tamaño es de 1,6 MB y su extensión es *.bmp* un formato del ITSL imagen de mapa de bits. La Figura 1 muestra el contenido gráfico de dicha imagen.

Figura 1. Descripción gráfica del fichero "*pista.bmp*"

- Un vídeo denominado "*lugar*" en formato *.mp4* y tamaño 172,2 MB extraído de la popular red social *Tik Tok*. La Figura 2 muestra parte del contenido gráfico de dicho vídeo.

Figura 2. Descripción gráfica de parte del fichero "*lugar.mp4*"

- Un fichero de tráfico de red denominado "*conversación*" cuya extensión es *.pcapng*. Este fichero contiene información relativa a la comunicación de red entre dos ordenadores. La Figura 3 muestra el contenido del tráfico de red generado entre dos ordenadores.

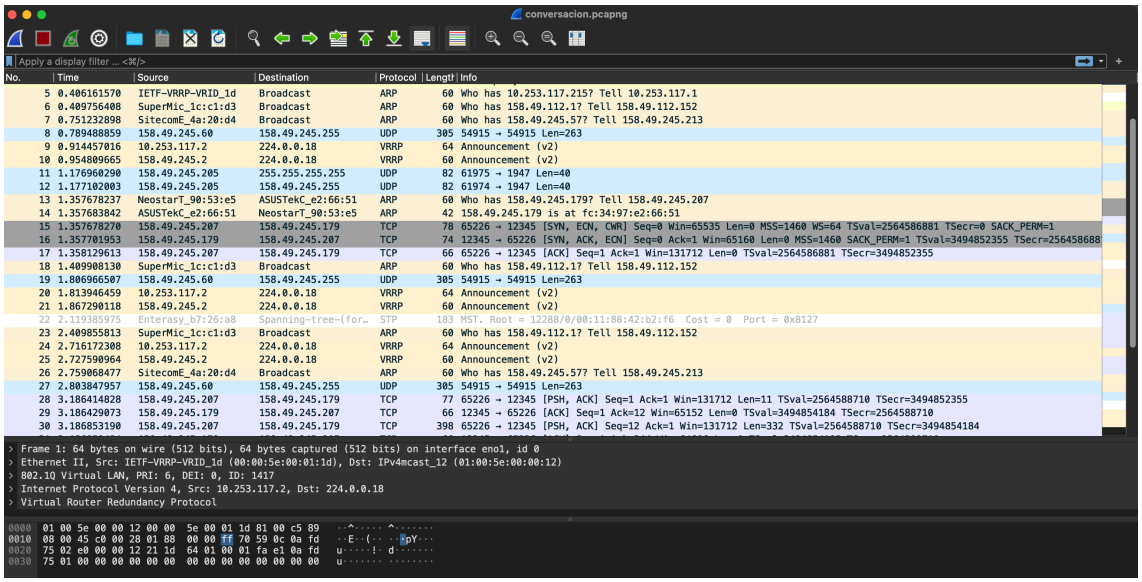

Figura 3. Descripción gráfica de la imagen contenida en el fichero *"conversacion.pcapng"*.

4. Conceptos básicos

Como se ha indicado en la introducción de la práctica se estudiarán los siguientes conceptos:

- **Esteganografía**: El término esteganografía proviene de las palabras griegas *steamos* (oculto) y *graphos* (escritura). Es una técnica que permite ocultar un fichero dentro de otro, o mensajes camuflados dentro de un objeto o contenedor, de forma que a simple vista no se detecte su presencia y consigan pasar desapercibidos.
- **Criptografía**: La criptografía proviene de las palabras griegas *kryptós* (secreto) y *graphé* (escritura), es la técnica que se ocupa de cifrar o codificar representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Existen multitud de tipos de cifrado como los *césar* y de rotación.
- **Técnicas de OSINT**: Muy de moda en profesionales de la Seguridad, la Inteligencia y el Periodismo, se denomina OSINT a la información -o inteligencia- obtenida de fuentes abiertas y que está disponible para cualquier usuario, sin restricciones de ningún tipo. Lo más importante de estas técnicas es la relación que puede ir resultando de la información obtenida.

5. Sesiones

Este apartado explica de manera resumida la planificación de las sesiones y las acciones a realizar dentro de cada una de ellas.

5.1. Sesión 1 – Resuelve el reto

- Al inicio de la sesión se realiza una explicación de la práctica, los conceptos básicos sobre los que trata la práctica, el contenido de las sesiones y la forma de entrega para la documentación.
- Durante esta sesión el estudiante sigue el procedimiento facilitado en el fichero "**Sesión 1 – Resuelve el reto.pdf**" para resolver el reto propuesto por el profesor. Se deben seguir los pasos minuciosamente para ir extrayendo la información de manera adecuada. Si el estudiante lo estima oportuno puede utilizar otras herramientas para llegar a la solución.
- **Sin entrega**: No es necesario que el estudiante entregue la resolución del reto.

5.2. Sesión 2 – Construye tu reto

- En la segunda sesión el estudiante diseñará y creará su propio reto. Podrá basarse en los mismos pasos y conceptos explicados durante la práctica (esteganografía, criptografía y técnicas de OSINT) o basarse en otros distintos. Durante esta sesión el estudiante sigue el procedimiento facilitado en el fichero "**Sesión 2 – Construye tu reto.pdf**"
  - El reto propuesto debe contener al menos tres pasos:
    - 1- Ocultar información en ficheros.
    - 2- Cifrar información utilizando cualquier tipo de cifrado *césar* o por desplazamiento.
    - 3- Extraer información útil de fuentes abiertas en Internet.
    - Se valorará la creatividad y las técnicas utilizadas para la creación del reto.
- **Entrega**: Al finalizar la semana o como muy tarde antes del comienzo de la tercera sesión, el estudiante debe disponer de su reto totalmente creado para poder enviárselo a otro compañero/a al inicio de la tercera sesión.

  ***Es importante ir generando una buena documentación durante la construcción del reto. Ya que la entrega de la documentación consistirá en explicar cómo se diseñado y creado el reto y, posteriormente, cómo se resuelve.

5.3. Sesión 3 – Resuelve el reto de otro compañero/a

- Durante la tercera sesión los estudiantes recibirán un reto creado por otros compañeros e intentarán resolverlo. Deberán analizar la información que les facilitan sus compañeros e intentar llegar a la solución.
- **Entrega opcional**: No es necesario que el estudiante entregue la resolución del reto propuesto por otro compañero/a. Sin embargo, de manera optativa se permite que el estudiante incluya en su documentación un apartado (marcando con la imagen ***bonus*** como se explicará posteriormente) con la resolución del reto de otro compañero.

6. Entrega y documentación

En este apartado se detallan los documentos que se deben entregar a través del aula virtual y cómo debe describirse la documentación que el estudiante debe aportar.

Es necesario entregar dos ficheros en el aula virtual:

1- El fichero denominado "**Reto_InicialesApellido1_InicialesApellido2_Nombre.zip**" comprimido con los datos del estudiante debe contener los materiales del reto. Este fichero debe contener a sus vez dos carpetas con los ficheros o información original y otra con los ficheros o información manipulada.

2- El fichero denominado "**CTF_InicialesApellido1_InicialesApellido2_Nombre.pdf**" en formato .pdf con la documentación de la práctica, con los apartados que se indican a continuación:

- **Portada** con el nombre del reto y los datos personales del estudiante. De manera optativa se podrá poner una imagen identificativa del reto.
- **Índice de contenidos** que contenga los apartados más importantes del documento junto con la página donde se encuentran.
- **Descripción del reto** y de los **conceptos** que se aplican en el reto.
- **Descripción del procedimiento** seguido para **diseñar y construir el reto** que contenga al menos:
    - Descripción de los **pasos para crear** el reto.
    - **Herramientas** utilizadas **para crear el reto** junto con una pequeña descripción.
- **Descripción del procedimiento** seguido de **resolución del reto** construido por los estudiantes.
    - Descripción de los **pasos para resolver** el reto.
    - **Herramientas** utilizadas **para resolver el reto** junto con una pequeña descripción.
- Es aconsejable que los estudiantes sigan la siguientes pautas básicas de redacción en el desarrollo de su documentación:
    - Escribir el documento utilizando **formas impersonales en tercera persona**. Por ejemplo: "se indica", "se detalla", "se explica", "se extrae".
    - **Identificar las figuras** con una nomenclatura básica y **referenciarlas en el texto** de manera descriptiva.
    - Diferenciar los términos en inglés con formato en *cursiva*.

7. Bonus

Los nuevos aspectos, cuestiones o conceptos que el estudiante incluya durante el desarrollo de la práctica pero que no se hayan visto con anterioridad y se encuentren debidamente descritos serán identificados con la imagen de ***bonus***. Esta tarea realizada por el estudiante se califica en el ítem de creatividad siguiendo las especificaciones de la rúbrica de evaluación de la práctica.

A continuación, se facilitan una serie de ideas que podrían servir para mejorar este apartado.

El estudiante puede innovar incluyendo en su reto nuevos conceptos que no se han explicado en la práctica pero que se encuentran relacionados con otras disciplinas de la informática como son:

- Ingeniería inversa.
- Exploiting.
- Análisis Forense.
- Hacking web.

Del mismo modo para la creación o resolución del reto puede incluir herramientas distintas a las incluidas por los profesores en las prácticas.

Otra de las cuestiones que puede considerarse interesante es que el reto esté acompañado de una historia que contextualice el reto en una situación real o ficticia.

Por último, también será considerado trabajo extra documentar la resolución del reto del compañero entregado.

7.1 ¿Cómo incluyo el bonus en mi documentación?

El estudiante debe colocar la imagen de ***bonus*** dentro de la documentación justo al lado del aspecto novedoso que implemente dentro de su práctica, junto con la descripción que detalle la razón de uso. Tal y como aparece en este apartado.

Los aspectos innovadores que se incluyan en la práctica que no se encuentren identificados con esta imagen no será valorados.

8. Evaluación

Las prácticas entregadas serán evaluadas de acuerdo a la rúbrica detallada a continuación:

Ítem	Valoración				
	Muy buena (2,5 puntos)	**Buena** (1,5 puntos)	**Regular** (0,5 puntos)	**Mala** (0 puntos)	**Ponderación**
Construcción del reto	Para crear el reto se hace un uso correcto de los conceptos explicados en la práctica: esteganografía, criptografía y técnicas de OSINT. Se describen de manera clara, concisa y apoyada de herramientas los pasos a seguir para crear el reto.	Para crear el reto se hace un uso correcto de los conceptos explicados en la práctica: esteganografía, criptografía y técnicas de OSINT. Se describen de manera clara y concisa los pasos a seguir para crear el reto, pero no se apoya en herramientas.	Para crear el reto no se hace uso de los conceptos explicados en la práctica: esteganografía, criptografía y técnicas de OSINT. No se describen de manera clara, concisa y apoyada de herramientas los pasos a seguir para crear el reto.	Para crear el reto no se hace uso correcto de los conceptos explicados en la práctica: esteganografía, criptografía y técnicas de OSINT.	**25%** **(*)**
Solución del reto	Se describen de manera clara y concisa los pasos a seguir para resolver el reto. Los pasos se apoyan en la descripción detallada del uso de las herramientas.	Se describen de manera clara y concisa los pasos que se deben seguir para resolver el reto, pero no se acompañan del proceso descriptivo para usar las herramientas que lo resuelven.	Se describen de manera clara y pero poco concisa los pasos que se deben seguir para resolver el reto. Solo se listan las herramientas que lo resuelven sin detallar su uso.	Se describen de manera poco clara y concisa los pasos que se deben seguir para resolver el reto, sin indicar las herramientas utilizadas.	**25%** **(*)**
Documentación	La documentación contiene todos los apartados indicados y se desarrolla siguiendo todas las pautas de redacción que se indican en la práctica.	La documentación contiene todos los apartados indicados y se desarrolla siguiendo varias de las pautas establecidas para la redacción pero no se siguen todas al completo.	La documentación contiene todos los apartados indicados y se desarrolla siguiendo solo alguna pauta de las establecidas para la redacción de la práctica.	La documentación no contiene todos los apartados y se desarrolla sin seguir las pautas de redacción que se indican en la práctica.	**25%**
Creatividad	Utiliza el ***bonus*** tres durante la práctica.	Utiliza el ***bonus*** dos veces durante la práctica.	Utiliza el ***bonus*** una vez durante la práctica.	No utiliza el ***bonus*** durante la práctica.	**25%**

(*) La suma de ambos apartados tendrá que ser igual o superior a 3 puntos. En caso contrario al calificación de la práctica será de Suspenso 3.