Penetration Testing

Seguridad en Sistemas Informáticos

Sebastian.Reyes@uclm.es

Curso 2020/21

Las pruebas de penetración (*Penetration Testing*) pueden definirse como un intento legal y autorizado para localizar y explotar con éxito sistemas informáticos con el propósito de hacer dichos sistemas más seguros. El proceso incluye sondear en busca de vulnerabilidades y llevar a cabo ataques que demuestren que existen riegos reales. Las pruebas siempre terminan con recomendaciones específicas para abordar y solucionar los problemas que se descubrieron durante la prueba de concepto (*Proof of Concept*, PoC). La idea general es encontrar problemas de seguridad mediante el uso de las mismas herramientas y técnicas que utilizan los atacantes.

Para la realización del PoC se utilizará el *framework Metaexploit* (disponible en la distribución *Kali Linux*) y la guía Approaching a Penetration Test Using Metasploit. En la guía se detalla el ciclo de vida de una prueba de penetración y se muestran varios ejemplos de *exploit*.

El trabajo consiste en la elección, análisis, descripción y demostración (PoC; *exploit*) de una vulnerabilidad con CVE (*Common Vulnerabilities and Exposure*). La elección debe notificarse con una respuesta a un mensaje del foro Cuestiones. La elección de un CVE (*exploit*) debe ser única. Para la elección del *exploit* se recomienda la revisión de alguna de las bases de datos de vulnerabilidades que hay disponibles en *Internet* como es el caso de **VULNERABILITY & EXPLOIT DATABASE** (**es conveniente revisar los trabajos, en el foro de la asignatura, que han sido elegidos por los compañer@s antes de llevar a cabo esta tarea**).

El trabajo constará de una memoria (en formato pdf, cuya estructura será la recomendada para los TFG y no podrá exceder de 25 páginas) y una presentación oral en clase o un vídeo explicativo (se recomienda prestar especial atención a la calidad del audio) cuya duración estará entre 5 y 10 minutos en el que se incluirá, necesariamente, la explicación y la demostración de la PoC.

La entrega será mediante una tarea en *moodle* y constará de un único archivo con el siguiente formato: Grupo_Letra.zip. El archivo deberá incluir:

- Si se ha optado por la presentación oral en clase (Evaluación continua; EC): la memoria y las transparencias, que se utilizarán como guía, para la defensa en clase. El plazo de entrega finaliza a las 00:00 del 14 de diciembre de 2020.
- Si se ha optado por la presentación oral en vídeo (Evaluación NO continua; ENC): la memoria y un enlace al sitio donde esté alojado el vídeo. El vídeo será alojado en un servidor público (en la nube) y debe estar disponible, para su **descarga**, hasta la fecha de cierre de actas de la convocatoria ordinaria (9-2-2020). El vídeo debe comenzar con una presentación de los autores. El plazo de entrega finaliza a las 00:00 del 18 de enero de 2021.

No se aceptarán entregas por ningún otro medio, ni fuera de plazo.

No se corregirán aquellos trabajos que traten sobre el mismo CVE o que hayan sido presentados en cursos anteriores.

La puntuación del trabajo será de hasta 25 puntos distribuidos de la siguiente forma: hasta 15 del trabajo en grupo (hasta 5 por el contenido de la memoria; hasta 5 puntos por el análisis del *exploit*; hasta 5 puntos por la demostración del *exploit*); hasta 10 puntos de presentación oral.