[Curso de Fundamentos de Pentesting](https://platzi.com/clases/pentesting/)

**ArtículoModelo de trabajo PTES**

[**Juan Pablo Caro**](https://platzi.com/%40juanpcaro)

12 de Agosto de 2019

En la clase anterior hablamos de un modelo de Pentesting en 4 etapas, el cual nos ayuda no solo a entender claramente el proceso de una prueba de penetración, sino a tener presente las actividades que deben hacerse a lo largo del proceso.

Si bien durante el curso vamos a trabajar con ese modelo de 4 etapas, es importante conocer otro modelo que se usa como referencia especialmente en contextos académicos: el **Modelo de Ejecución Estándar de Pruebas de Penetración, o PTES (Penetration Testing Execution Standard).**

**La estructura general del PTES define siete secciones o pasos como la base para la ejecución de un proceso de Pentesting:**

**Interacción previa**

Esta fase hace referencia a la **preparación previa al inicio del proceso de Pentesting** como tal, particularmente en la definición de alcance, tiempo y necesidades con el cliente. Es importante tener en cuenta factores y preguntas como:

* Horario en el que se harán las pruebas.
* Cantidad de direcciones IP a probar.
* Pruebas sobre equipos que deben estar disponibles.

**Recolección de información**

Esta fase corresponde a la misma etapa que estudiaremos en el curso. El propósito es **recopilar toda la información posible** sobre los objetivos que serán probados durante el pentesting.

**Modelo de amenazas**

El estándar PTES define una etapa de modelo de amenazas con el fin de hacer más eficiente el proceso completo. En esta etapa se considera, a partir del contexto particular del cliente, **cuáles son los riesgos y las amenazas más probables a las que está expuesto, y los bienes o activos que más debería proteger.**

**Análisis de vulnerabilidades**

Durante este proceso vamos a identificar los posibles fallos de seguridad que puedan ser aprovechados por un atacante. Esta fase la estudiaremos en detalle durante este curso.

**Explotación**

El objetivo principal de la fase de explotación es **ganar acceso a algún sistema o dispositivo aprovechando las fallas de seguridad encontradas en la fase anterior**. Una particularidad de la fase de explotación es que las estrategias, técnicas o fallas aprovechadas pueden variar dependiendo del sistema en particular que sea analizado.

**Post-Explotación**

Una vez ganado el acceso a un sistema, es posible que se requiera **mantener este acceso para continuar avanzando dentro del entorno**, para obtener información posteriormente o hacer actividades de monitoreo.

**Reporte**

Si bien no lo incluimos como una fase de nuestro proceso, la etapa final de todo proceso de pentesting debe ser la **elaboración de un reporte a partir de la información recolectada**, las fallas identificadas y explotadas y la información sensible obtenida. Para la elaboración de este informe generalmente se recomienda elaborar un mapa de riesgos con una escala de valor, y generar un informe ejecutivo que resuma los resultados obtenidos.

Reportar un problema

**Instalación y configuración de máquinas virtuales para laboratorios**