Caso Práctico

Parte 1

Identificar y explotar el mayor número de vulnerabilidades en la máquina Metasploitable que puede descargarse del siguiente enlace.

https://drive.google.com/file/d/1Z_m9RgCUN4McvcFpmlZjfYtdUTLZSoif/view?usp=sharing

El entregable será un informe con una lista de vulnerabilidades. Para cada una de ellas hay que rellenarlas con los siguientes campos:

- Descripción: En que consiste el fallo de seguridad.
- Impacto: Cual es el peligro/impacto de explotar esta vulnerabilidad.
- Explotación: Explicación paso a paso seguido en la identificación y explotación y de la vulnerabilidad. El receptor del informe (en el mundo real el cliente que te ha contratado) tiene que ser capaz de reproducir tus pasos.
- Mitigación: Breve explicación de como solucionar el fallo (1 o 2 lineas podrian ser suficientes en muchos casos).

Parte 2

Identificar y explotar el mayor número de vulnerabilidades en la aplicación web Badstore que se encuentra en el siguiente enlace:

https://drive.google.com/file/d/1DzkH-YT0pLpKXkg837Tma5EMiX0BKGJI/view?usp=sharing

El fichero es una ISO. Hay que crear una máquina virtual Debian 9 64bits y seleccionar la ISO como disco instalador.

El entregable será un informe con una lista de vulnerabilidades. Para cada una de ellas hay que rellenarlas con los siguientes campos:

- Descripción: En que consiste el fallo de seguridad.
- Impacto: Cual es el peligro/impacto de explotar esta vulnerabilidad.
- Explotación: Explicación paso a paso seguido en la identificación y explotación y de la vulnerabilidad. El receptor del informe (en el mundo real el cliente que te ha contratado) tiene que ser capaz de reproducir tus pasos.
- Mitigación: Breve explicación de como solucionar el fallo (1 o 2 lineas podrian ser suficientes en muchos casos).