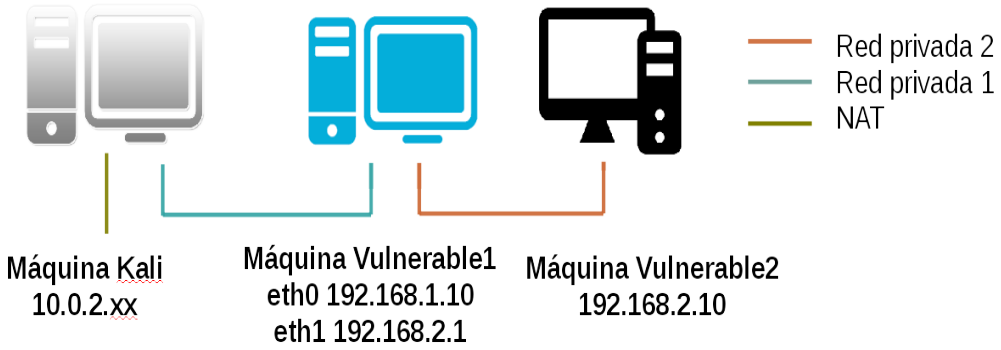
SCHOOL OF HACKING 2015
RETO METASPLOIT-ARMITAGE

ENTORNO PARA LOS EJERCICIOS

Para la resolución del reto habrá que tener instaladas una serie de máquinas virtuales similar a la utilizada en el correspondiente Taller: una de ellas configurada como la máquina atacante, con Kali, y las otras como máquinas vulnerables.

Esta ABSOLUTAMENTE PROHIBIDO realizar escaneos, pruebas, y ataques contra cualquier máquina que no sea las contempladas en el supuesto del reto, es decir, fuera del entorno de virtualización.

La configuración de red y los sistemas vulnerables para los Ejercicios 3 y 4 se muestran en la Figura siguiente:



Las máquinas virtuales en formato *.ova* pueden descargarse de la URL: http://lsi.ugr.es/jagomez/RetoMetasploitArmitage.zip. La máquina Vulnerable1 puede descargarse de http://lsi.ugr.es/jagomez/Vulnerable1.ova.zip.

A partir del momento momento de la publicación se dispondrá hasta el miércoles 11 de marzo a las 24:00 horas como plazo máximo para la entrega.

Cuando se hayan resuelto los ejercicios deberá mandar un correo electrónico, a una de las direcciones siguientes jagomez@ugr.es o afdiaz@ugr.es, conteniendo de forma breve y clara la solución de los ejercicios. Sólo se aceptará una una solución por participante. La puntuación máxima la obtendrá el primero que remita la solución correcta y a partir de ese momento se irá decrementando la puntuación en 1 punto.

EJERCICIOS PUNTUABLES

3.- (**PUNTUACIÓN: 5 Puntos**) Explotar una vulnerabilidad de la máquina *Vulnerable1* que tiene como dirección 102.168.1.10 con `msfconsole`.

3.1.- Qué vulnerabilidad se va a atacar para tener acceso de *root*.

3.2.- Cómo se ha atacado.

4.- (**PUNTUACIÓN: 15 Puntos**) El objetivo es extraer un fichero oculto del usuario *pepe* en la máquina *Vulnerable2*. Para ello debe pasar a través de la máquina *Vulnerable1*.

Describir todos los pasos seguidos para la extracción del fichero oculto, indicando el nombre

descifrado del mismo y una captura de su contenido.