SCHOOL OF HACKING 2015
RETO METASPLOIT-ARMITAGE

INSTRUCCIONES

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.

La configuración de red y los sistemas vulnerables para los Ejercicios 3 y 4 se darán a conocer por correo electrónico a los participantes inscritos durante el lunes 9 de marzo. A partir de ese momento se dispondrá de dos días para su resolución y entrega de las soluciones, que finalizará el 11 de marzo a las 24:00 horas.

Hay dos ejercicios que puntuaran para la consecución del reto. Cuando el participante crea haber resuelto estos ejercicios deberá mandar un correo electrónico a la dirección jagomez@ugr.es para la solución del Ejercicio 3, y a afdiaz@ugr.es para el Ejercicio 4, conteniendo de forma breve y clara la solución de los ejercicios. Sólo se aceptará una una solución por participante. La puntuación se obtendrá por el orden en el que se remiten las soluciones correctas.

EJERCICIOS

Las actividades a realizar son:

1.- Configurar un entorno similar al visto en el Taller tanto en la parte de `msfconsole` como la de `armitage`.

2.- Probar las explotación de los sistemas vulnerables configurados en un entorno de pruebas configurado por vosotros, explorando las diferentes posibilidades de las herramientas.

3.- (**PUNTUACIÓN: 5 Puntos**) Explotar una vulnerabilidad de una máquina A que se fijará como objetivo cuando se abra el Reto con `msfconsole`.

4.- (**PUNTUACIÓN: 15 Puntos**) Explotar una vulnerabilidad de una máquina B que se fijará como objetivo cuando se abra el Reto.