Explotación del Servicio http Apache Tomcat del puerto 8081.

Escaneo de la ip víctima.

Escaneo del puerto 8081, vemos que es un servicio http Apache Tomcat 5.5

En msf buscamos apache 5.5

Elegimos un exploit que ya viene con un payload configurado.

Ingresamos ip y puerto victima.

Buscamos en google credenciales por default para apache tomcat 5.5, ingresamos en un resultado de github. Seleccionamos una opción, copiamos y seteamos en la terminal el username y password con esas credenciales.

Corremos el comando exploit.

Conseguimos una sesión abierta a metasploitable.