EJERCICIOS INTRODUCCIÓN A LA POST-EXPLOTACIÓN Y PERSISTENCIA

Prerrequisitos

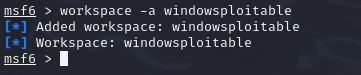
Kali Linux

Windowsploitable

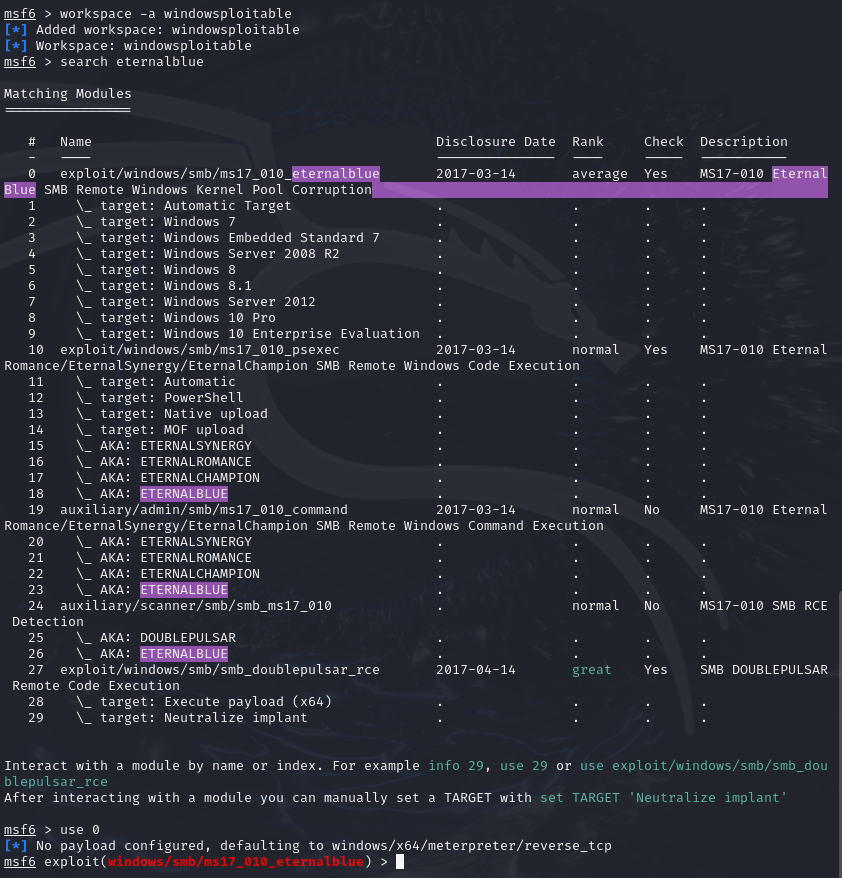
Metasploitable2

Ejercicio 1 - Metasploit

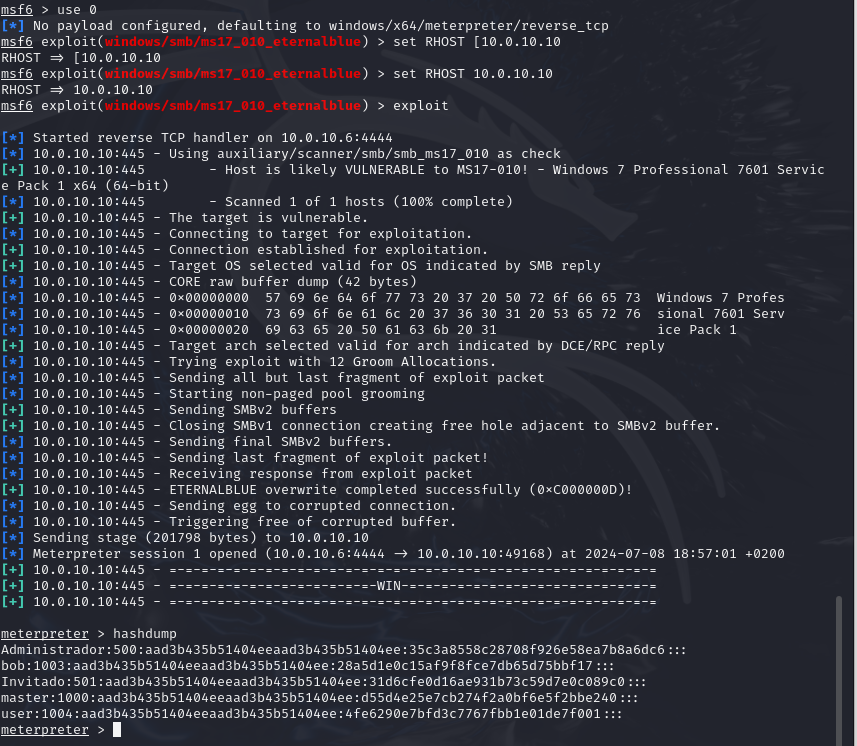
Crear un workspace para la siguiente auditoría con el nombre Windowsploitable.



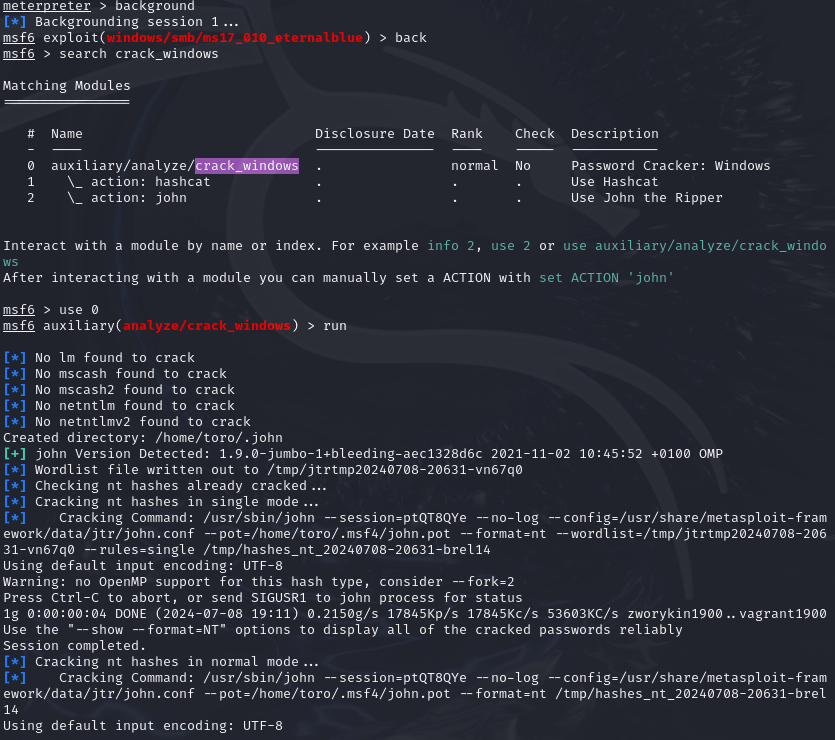
Explotar la vulnerabilidad EternalBlue usando un payload meterpreter.

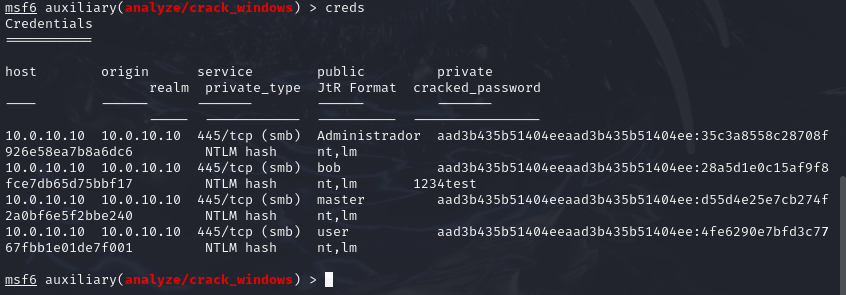


Volcar los hashes con comando meterpreter, o módulo de post-explotación de ser necesario.

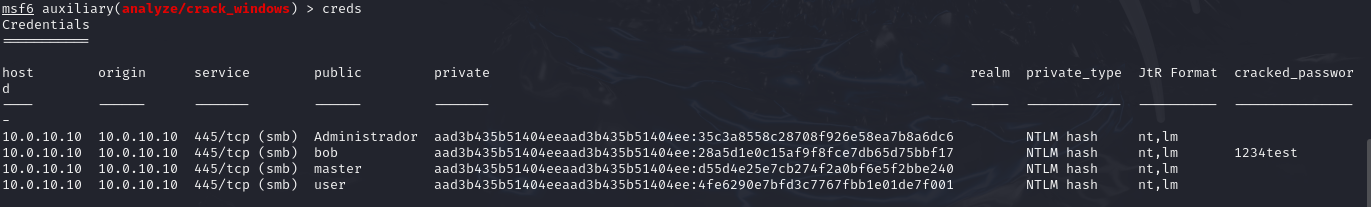


Comprobar que las credenciales estan añadidas a nuestro workspace.





Crackear los hashes almacenados usando el módulo destinado a ello.



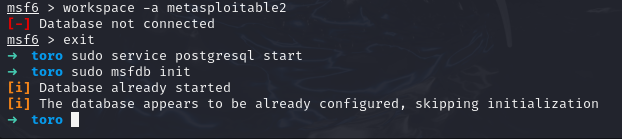
Hacer persistencia y demostrar su funcionamiento reiniciando el sistema.

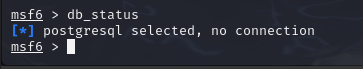
hasta aquí lo he echo en clase, pero no he podido terminarlo en casa en cuanto, como

ya comentado en el ejercicio precedente, no he podido acceder a la maquina windows… :-(

Ejercicio 2 - Metasploit

Crear un workspace para la siguiente auditoría con el nombre Metasploitable2.





nada, no ha habido manera de poder conectar la base de datos, lo he intentado todo comprendido la modificación de los ficheros “database.yml”, “pg\_hba.conf” y creando nuevos usuario y base de datos.

de todas formas los pasos para hacer este ejercicio se asemejan al primero y seria como hacer una repetición, en cualquier caso en clase veo se puedo terminarlo utilizando otro ordenador… ;-)

Explotar la vulnerabilidad Java\_RMI usando un payload meterpreter.

Volcar los hashes con comando meterpreter, o módulo de post-explotación de ser necesario.

Comprobar que las credenciales estan añadidas a nuestro workspace.

Crackear los hashes almacenados usando el módulo destinado a ello.

Hacer persistencia y demostrar su funcionamiento reiniciando el sistema.