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

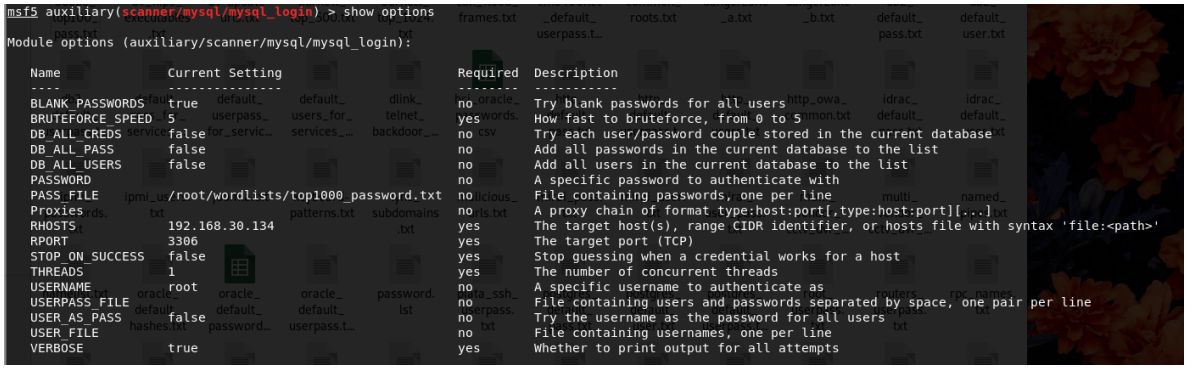
3、vnc服务：
VNC (Virtual Network Console)是虚拟网络控制台的缩写，是一款远程控制工具。
• 默认端口：5900
• 模块位置：auxiliary/scanner/vnc/vnc_login
4、samba服务：
Samba是在Linux和UNIX系统上实现SMB协议的一个免费软件，是一种在局域网上共享文件和打印机的一种通
信协议。
• 默认端口：445
• 模块位置：auxiliary/scanner/smb/smb_login

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

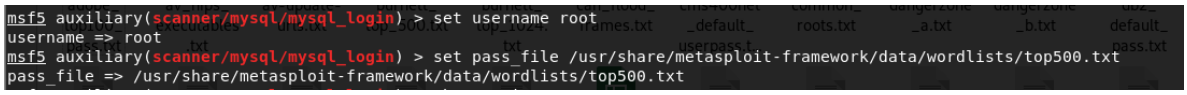
使用mysql口令破解模块

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

查看选项

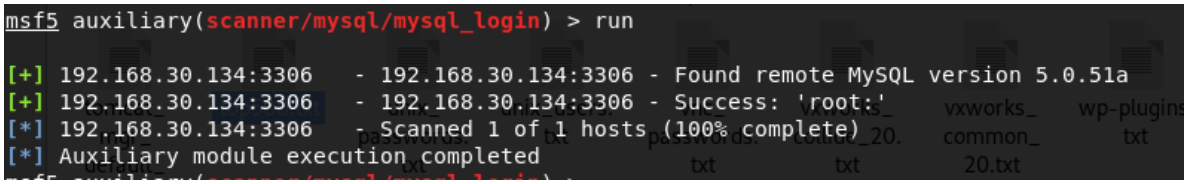


填写选项



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

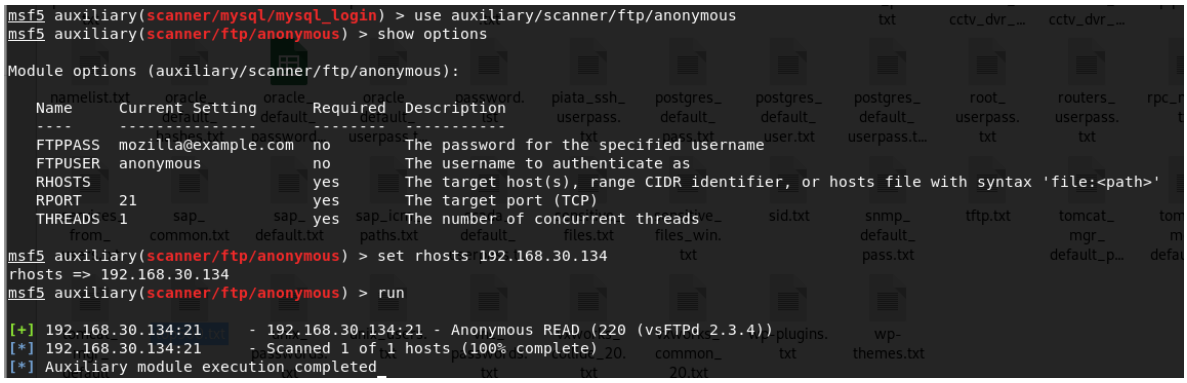


7、mssql服务：
Mssql（sql server）是一个关系型数据库管理系统，使用sa登录之后可以使用xp_cmdshell执行系统命令。
• 默认端口：1433
• 模块位置：auxiliary/scanner/mssql/mssql_login
8、oracle服务：
oracle是一个关系型数据库管理系统。
• 默认端口：1521
• 模块位置：auxiliary/scanner/oracle/oracle_login

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



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