1.crunch命令（字典生成）

举例：crunch 1 5 G2sk -o /root/Desktop/a.txt

说明：最小位数1 最大位数5 且包含G2sk字符的字典，生成后保存在桌面的a.txt文件/root/Desktop/a.txt

2.dmitry命令（域名whois查询）

-o输出保存到％host.txt或文件通过-o指定的文件

  -i上的主机的IP地址执行WHOIS查询

  -w在主机的域名执行Whois查询

  -n检索主机上Netcraft.com信息

  -s执行可能的子域搜索

  -e执行对可能的电子邮件地址搜索

  -p执行主机上的TCP端口扫描

\*-f执行主机上的TCP端口扫描显示输出报告过滤的端口

\*-b读取来自扫描端口接收的旗帜

\*扫描TCP端口时-t0-9设置以秒为单位的TTL（默认值2）

\*需要标记要传递的-p

举例：dmitry -wnpb baidu.com

扫描域名为baidu.com下的whois信息

3.amap命令（服务器枚举指令）

举例：amap –bq 192.168.0.100 500-1000

检测ip为192.168.0.100的服务器的500到1000端口上开放的端口以及运行的服务

4.findmyhash(穷举破解指令)

举例：findmyhash MD5 –h e10adc3949ba59abbe56e057f20f883e

穷举破解密文类型为MD5的密文e10adc3949ba59abbe56e057f20f883e，过程较慢（推荐直接去CMD5），当然该命令也支持SHA1,SHA256等等