Hydra使用：

Hydra是一款由著名的黑客组织THC开发的开源暴力破解工具，支持大部分协议的在线密码破解，是网络安全·渗透测试必备的一款工具。

命令示例：

```
hydra -L user.txt -P passwd.txt -o ssh.txt -vV -t ip  ssh -s 22
-L 指定用户字典文件
-P 指定密码字典文件
-o 把成功的输出到ssh.txt文件
-vV 显示详细信息
-s 指定其他端口 如果要修改默认22端口，可以使用 -s 参数
```

```
参数：
-l login 小写，指定用户名进行破解
-L file 大写，指定用户的用户名字典
-p pass 小写，用于指定密码破解，很少使用，一般采用密码字典。
-P file 大写，用于指定密码字典。
-e ns 额外的选项，n：空密码试探，s：使用指定账户和密码试探
-M file 指定目标ip列表文件，批量破解。
-o file 指定结果输出文件
-f 找到第一对登录名或者密码的时候中止破解。
-t tasks 同时运行的线程数，默认是16
-w time 设置最大超时时间，单位
-v / -V 显示详细过程
-R 恢复爆破（如果破解中断了，下次执行 hydra -R /path/to/hydra.restore 就可以继续任务。）
-x 自定义密码。
service：指定服务名，支持的服务跟协议有：telnet，ftp，pop3等等。
注意：
1.自己创建字典,然后放在当前的目录下或者指定目录。
2.参数可以统一放在最后，格式比如hydra ip 服务 参数。
3.如果能确定用户名一项时候，比如web登录破解，直接用 -l就可以，然后剩余时间破解密码。
4.缺点，如果目标网站登录时候需要验证码就无法破解。
5.man hydra最万能。
6.或者hydra -U http-form等查看具体帮助。
```

例子：

```
破解ftp：
hydra -L 用户名字典 -P 密码字典 -t 6 -e ns IP地址 -v
```

http协议破解
get方式提交，破解web登录：

```
hydra -L 用户名字典 -P 密码字典 -t 线程 -v -e ns IP地址 http-get /admin/
hydra -L 用户名字典 -P 密码字典 -t 线程 -v -e ns -f IP地址 http-get /admin/index.php
```

post方式提交，破解web登录：

```
hydra -f -l 用户名 -P 密码字典 -V -s 9900 IP地址 http-post-form "/admin/index.php?action=login:user=USER&pw=PASS:"

#/index.php …这个是登录的 url
#后门是POST的数据 其中的用户名密码使用 USER PASS 来代替
#然后是如果登录出错 会出现的字符 。。。然后开始破解
```

破解https

```
hydra -m /index.php -l 用户名 -P 密码字典.txt IP地址 https
```