第5周周报

kali学习使用

第工具一个Nmap
通过扫描目标的IP地址或URL来收集信息的工具
首先要访问Nmap，在终端上输入Nmap 命令，然后输入要扫描的目标
$ nmap scanme.nmap.org

然后是一些我学到的基础的用法

1 扫描目标开放端口： nmap <目标IP> 例如： nmap 192.168.3.124 这将扫描目标IP的开放端口，并显示端口号、状态和运行的服务
漏洞扫描（我觉得用的最多的一个）： nmap --script=vuln <目标IP> 例如： nmap --script=vuln 192.168.3.124 这将扫描目标IP上的漏洞，并列出扫描结果
全面扫描： nmap -A <目标IP> 例如： nmap -A 192.168.3.124 这将扫描目标IP的操作系统信息、版本信息、路径跟踪等内容

指定端口扫描： nmap -p <端口号> <目标IP> 例如： nmap -p 445 192.168.3.124 这将扫描目标IP上的指定端口，速度更快
小结：name主要就是扫描，获取信息

sqlmap工具学习

“sqlmap是针对sql注入漏洞的一款自动化sql注入探测工具，支持多种操作系统环境和多种数据库的漏洞探测，渗透测试人员常常调侃“没有什么操作技术，就是sqlmap一把梭哈，屏幕显示绿了就直接下班”引用一下别人的话来理解这个工具

sqlmap的基本使用:

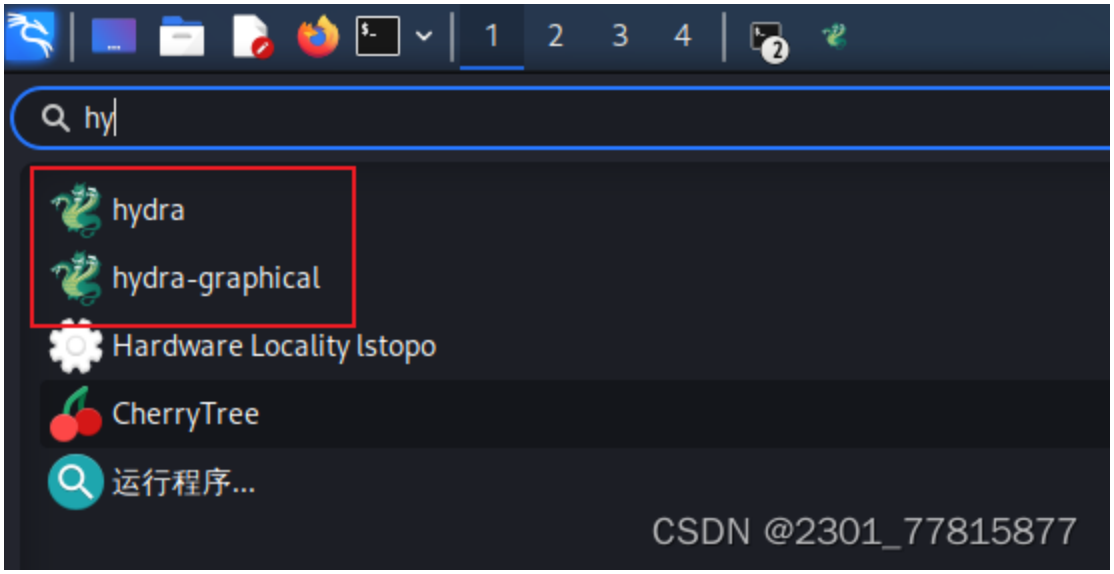
sqlmap -u "www.baidu.com"好吧，这个工具有些看不懂如何操作，待我后面上机实验试试

hydra

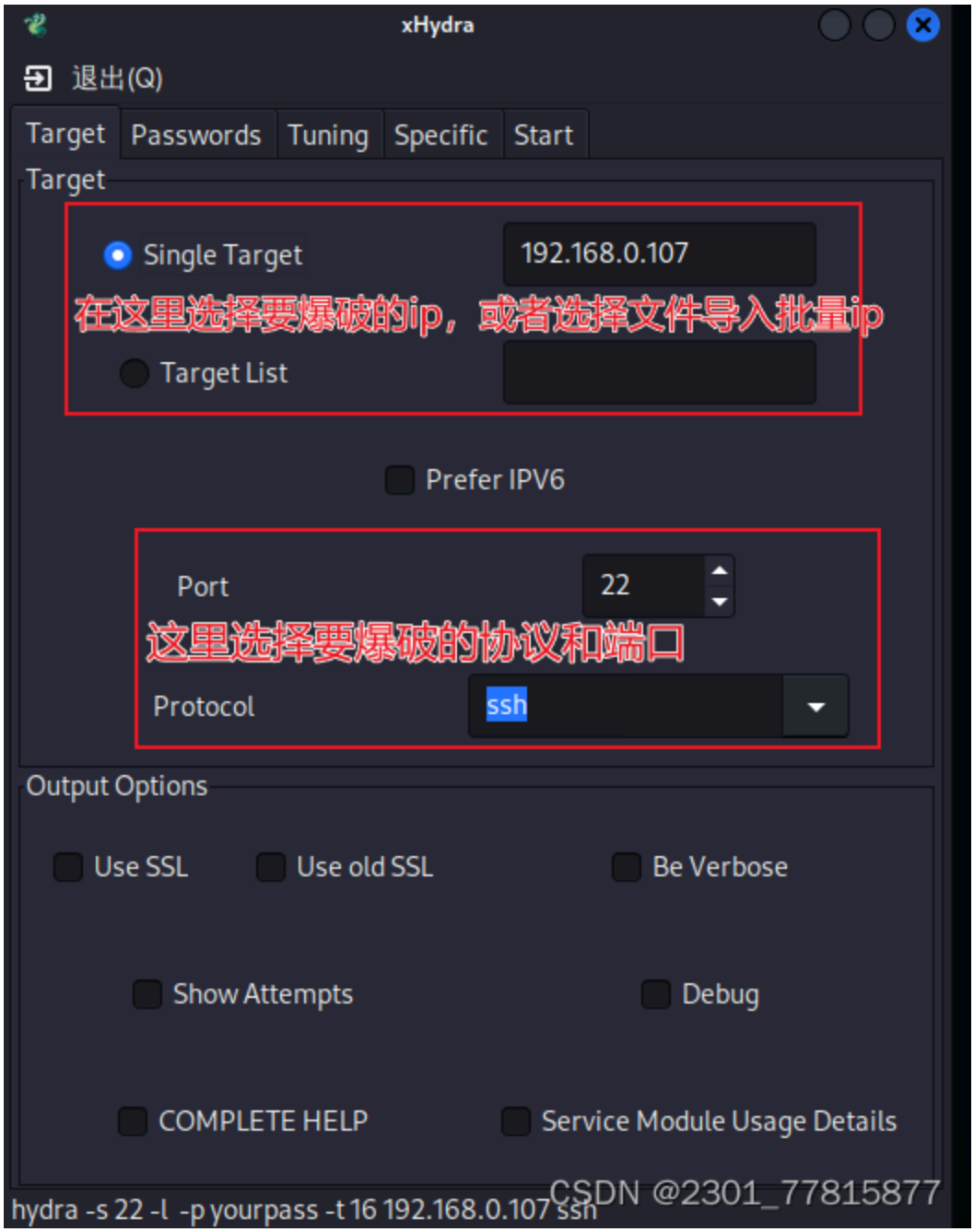
一个简单的的爆破工具

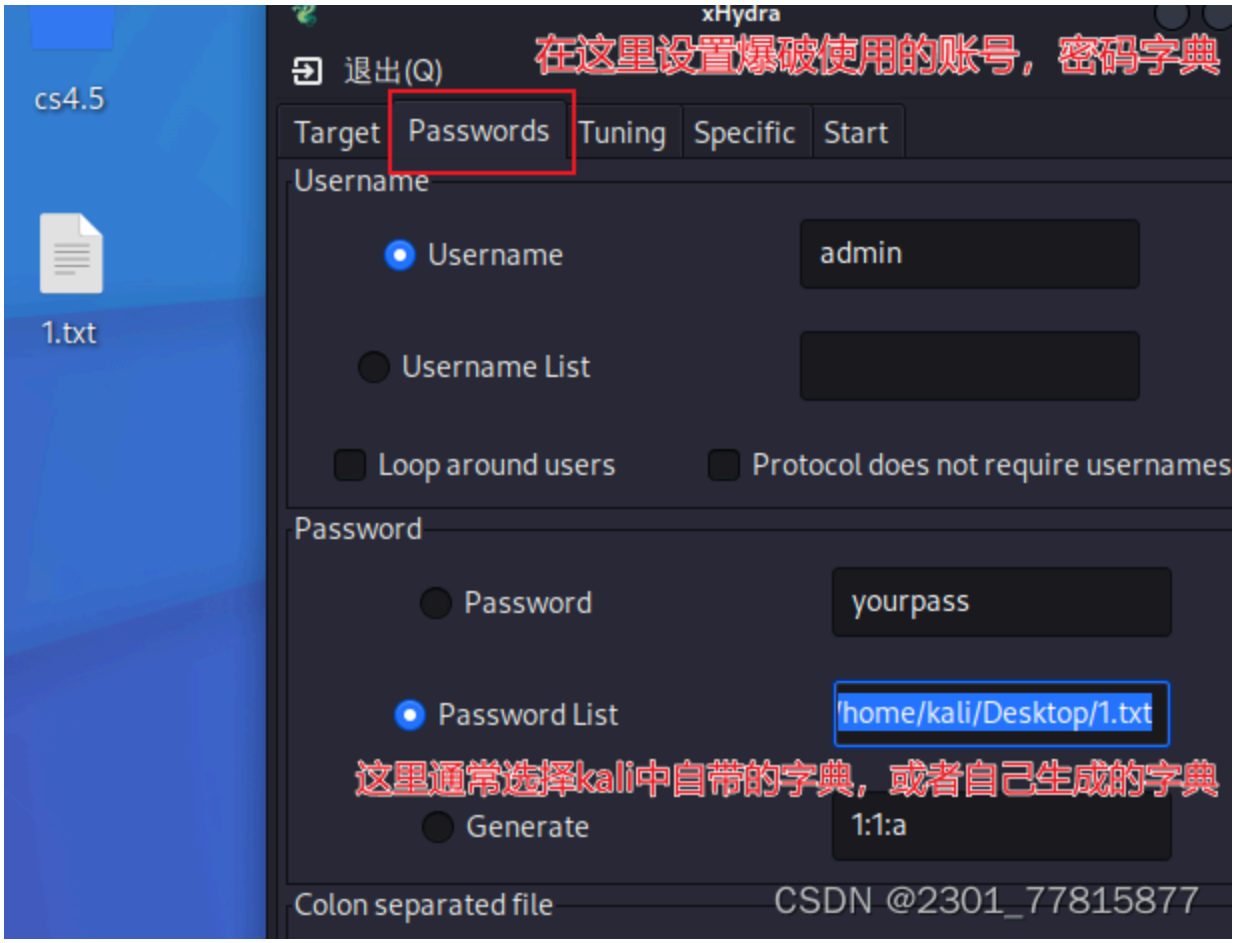
hydra又称九头蛇，是一款非常高效的多种协议都可以使用的爆破工具，对指定ip的指定服务进行爆破，需要输入爆破使用的字典或者自己指定爆破使用的数据（比如在已知账号为admin时爆破密码）

在kali中hydra有图形化和命令行两种使用方式



下面介绍图形化使用





之后选择start就好了，hydra会使用字典中的所有账号密码去做登陆的爆破尝试