Q：本文采用的ddos攻击的手段是什么

A：syn-flood和dns放大反射攻击

建议参考资料如下：

Syn-Flood：<https://www.jianshu.com/p/6eae45826754>

Dns-反射放大攻击：<https://cloud.tencent.com/developer/article/1463080>

Q：代码中用到的第三方库分别有什么

A：版本：python3.7

在该版本的python下只有scapy一个第三方库

若是其他版本的python可能由于标准库不同导致有些库缺失，只需要在终端pip install [相应的库名] 即可

Q：这些文件都有什么用 ？

A：DDOS攻击实质上是分布式的DOS攻击，分布式就是同时在多台主机运行，这些进行DOS攻击的主机被叫做肉鸡，控制肉鸡的主机叫做服务端。

所以需要提供服务端和肉鸡的连接以及控制

client.py ：部署在肉鸡上，连接服务端，接收服务端命令并执行

server.py : 部署在服务端上，接收肉鸡连接，向肉鸡发送命令

dos.py：部署在肉鸡上，也可单独运行对指定的目的ip和端口进 行dos攻击。

ddos.py：部署在被攻击主机上，检测ddos攻击，检测算法可以见参考论文，此处对论文里面的算法做出了适当改进。

Q：没有多台主机的情况下如何进行DDOS攻击？

A：修改dos.py中的随机生成的ip地址的数量，模拟ddos即可，无需严格的ddos攻击

Q：我应该攻击哪台主机

A：1.网络不是法外之地，请不要攻击商用服务器。

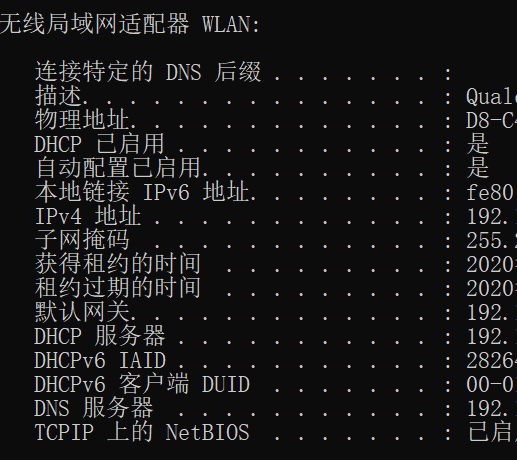
2.可以攻击自行购买的个人服务器

3.攻击个人虚拟机(建议为windows虚拟机)

Q：在代码中需要填入ip地址，我应该如何查看ip地址呢

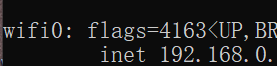
(server.py和dos.py都需要查看ip地址)

A：Windows下：打开cmd 输入 ipconfig /all ，下图圈起项为ip地 址





Linux下：打开终端，输入ifconfig，查看eth0或wifi0

 (此处为了保护隐私截图没有截全，inet后跟的所有数字才是ip地址)



Q：ddosCheck.py中的ddosMeasure和normalMeasure是如何得到的 ？

A：鉴于本人居家电脑性能有限，收集了在正常状态和ddos状态下10次数据，每次收集5000个包，然后计算两种情况下的每一次的4维信息熵，然后用10次的向量取平均所得。

Q：ddosCheck.py中的ddosMeasure和normalMeasure是如何得到的 ？

A：鉴于本人居家电脑性能有限，收集了在正常状态和ddos状态下10次数据，每次收集5000个包，然后计算两种情况下的每一次的4维信息熵，然后用10次的向量取平均所得。此处建议使用者自行利用封装好的函数进行测试并替换这两个结果，因为不同的ip适用的常量不同。

Q：python中用到了一个库scapy，应该在哪里学习这个库的内容？

A： <https://blog.csdn.net/a649344475/article/details/81110957?depth_1-utm_source=distribute.pc_relevant.none-task&utm_source=distribute.pc_relevant.none-task>

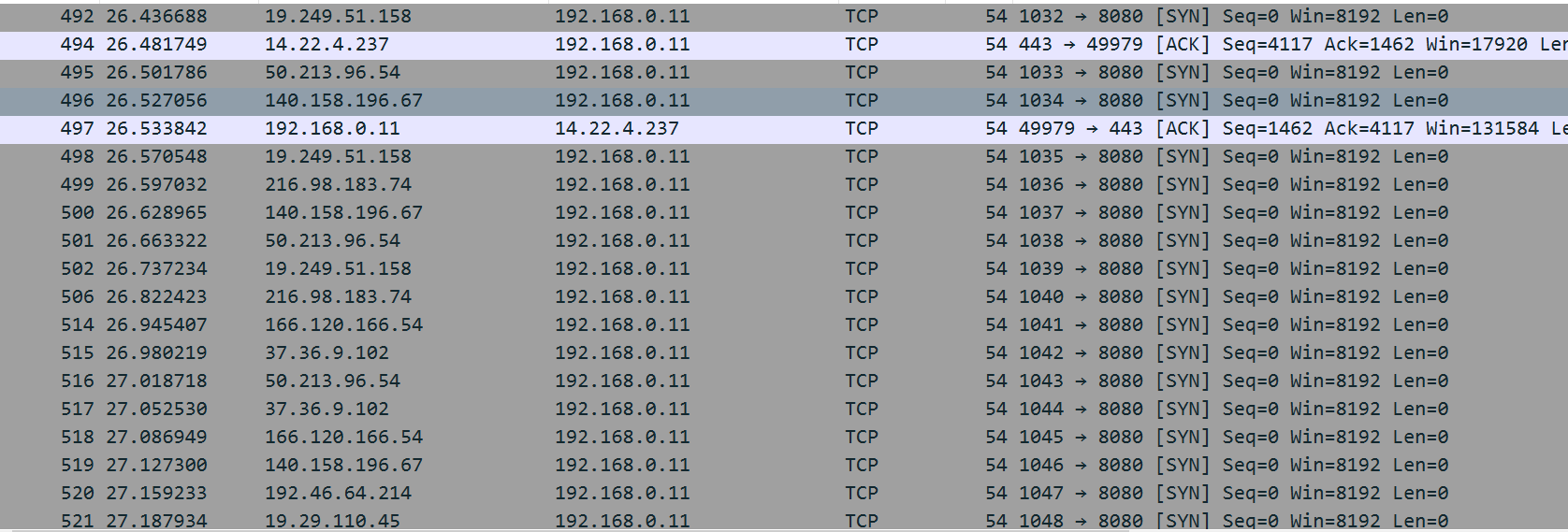
<https://nonuplebroken.com/2018/11/05/%E4%BD%BF%E7%94%A8python-scapy%E5%BA%93%E8%AF%BB%E5%8F%96wireshark%E6%95%B0%E6%8D%AE%E5%8C%85/>

<https://github.com/Larryxi/Scapy_zh-cn>

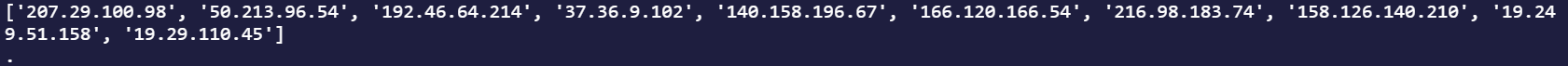
<http://blog.sina.com.cn/s/blog_4b5039210100fa1z.html>

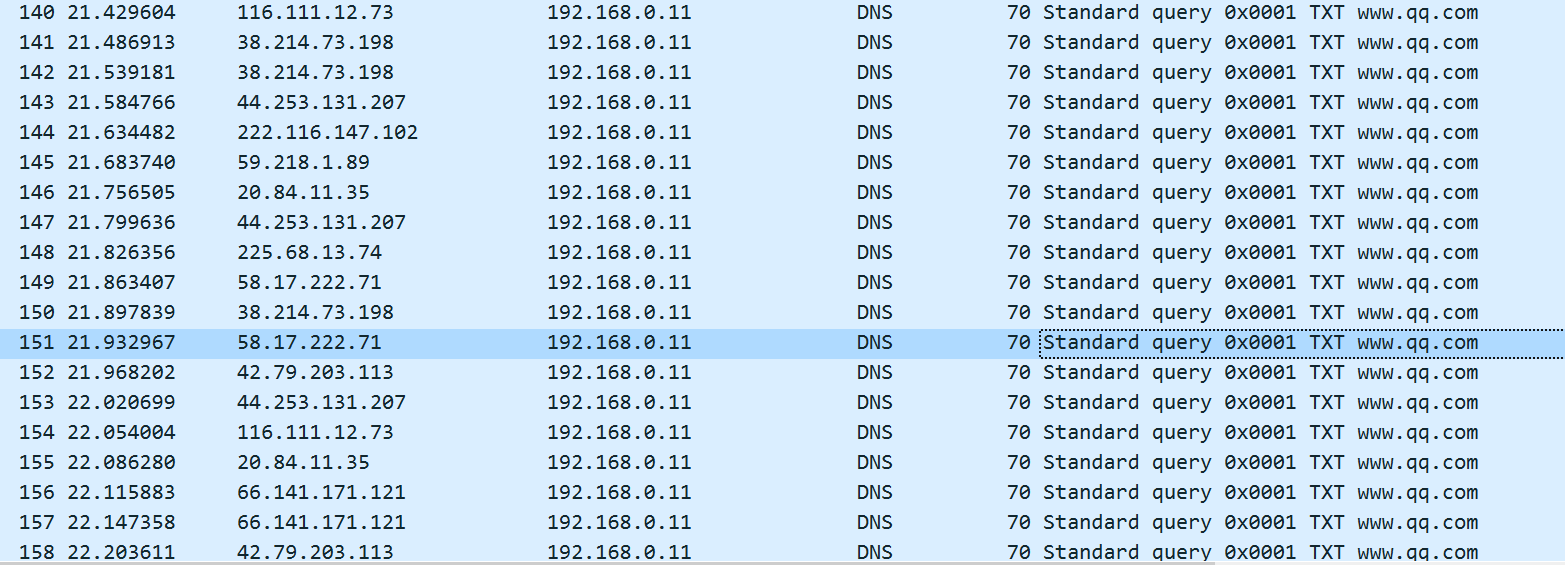
Q：遭受DDOS攻击时wireshark的截图的状态

A：以下是我在windows虚拟机中的截图

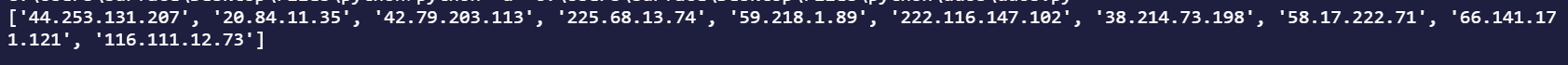


随机伪造的syn-flood攻击IP地址列表：





随机伪造的DNS反射放大攻击IP地址列表：



Q：还有哪些库需要学习的？

A：除了scapy内容太多注释写不完之外，其他的库的函数的作用都已经在注释中解释了。如果有不懂的话自行谷歌搜索

输入：XXXX python3 中文文档即可