**病毒检测与入侵第四次作业**

赵文博 软网1404 201492078

呼…不知不觉就到了最后一次作业了，作为结束，我想对之前实践中产生的疑问进行猜测或解答，这也算是这们课程最大的收获了吧。

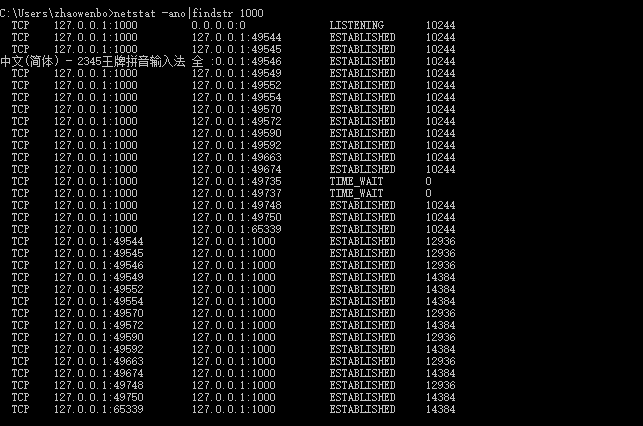
**Question 1: 157.240.0.17是最新hosts文件里的一个IP, 在替换系统hosts之前直接在浏览器输入https://157.240.0.17不能访问网站，是什么原因呢？**

猜想：在地址栏输入之后，通常出现的都是安全证书存在问题，联系第一次作业中提到的防火墙防御机制中有一个SSL证书过滤，很有可能使这一机制在搞鬼。

因为我们是通过IP地址访问的Facebook, 在访问之前我们并不知道域名，所以必须要通过访问获得SSL证书，而证书在传回来的过程中被防火墙过滤，从而产生了问题。但是如果修改过hosts文件，通过域名访问的话，由于已知要访问Facebook, 而本地又已经有了SSL证书，就不用在此获取。故而可以正常访问。

**Question 2: Shadowsocks 客户端里有两个端口，服务器端口和代理端口，分别指什么？**

上次我们已经看到了，服务器端口600在我们的客户端和服务器上都可以看到，并且已经建立了TCP连接，所以这里的服务器端口应该就是我们所访问的端口， 而默认的代理端口1080又是什么呢？网上的解释如下：这一协议以[通道方式](http://baike.baidu.com/view/3561891.htm)穿过防火墙，允许防火墙后面的人通过一个IP地址访问INTERNET。然而还是不明白是什么意思，于是我将1080端口改成了1000端口，然后再电脑上查看得到下图：



我们可以看到，源端口和目的端口都是本机的端口。个人理解可能就是本机的进程通过与1080端口通信就可以实现代理的目的，通过我们的防火墙吧。（不是很确定）

**Question 3：第二次作业中提到的在ipv4的网络环境中访问ipv6还有什么方式？**

之前我们提到，现在各个大学推广的ipv4 to ipv6使用的是isatap协议，然而这个协议不能用于NAT网络环境下，后来我又找到了一个微软公司推出的协议：Teredo协议，也是用于ipv4 to ipv6, 通过这个协议，我确实在ipv4网络中获取到了ipv6的地址，然而却发现ping 很多国内外的ipv6网站都不能成功，只有一个网站 ping -6 bgp.he.net ，在ipv4环境下不能成功，使用Teredo协议后成功了，网上有人说大部分网站已经把这个协议屏蔽了。。。

最后再给大家安利几个比较好用的翻墙软件

1. 蓝灯
2. XX-Net
3. 天行VPN
4. 网上的一些卖的Shadow socks服务器 IP 和端口。