病毒检测与入侵第二次作业

赵文博 软网1404 201492078

这次我们来谈一谈翻墙的方法之一

通过修改hosts 文件+https 的翻墙方式。

上回我们介绍了GFW的几种封锁方式，下面我们就修改hosts文件的方法来分析一下它究竟是如何实现翻墙的。

首先，对于IP封锁而言， 由于一个域名对应于很多个IP， 对于GFW而言，谷歌的IP是很难封锁完的，所以我们只要找到那些没有被GFW封锁的IP, 还是可以继续访问谷歌的。那么问题来了，怎么获得没有被墙掉的IP呢？一般是有网页获得的。 当位于国外的可以正常上谷歌的同胞们用谷歌搜索信息并跳转到相关网页上时，网页会记录来源网站（谷歌）的IP信息，经过选择就得到了我们所用的没有被墙掉的IP.我们可以通过ping IP地址的方式来检验IP是否被墙。

其次，对于域名污染/劫持，可以通过hosts文件解决，hosts文件的定义如下：Hosts是一个没有扩展名的系统文件，可以用记事本等工具打开，其作用就是将一些常用的网址[域名](http://baike.baidu.com/view/43.htm)与其对应的[IP地址](http://baike.baidu.com/view/3930.htm)建立一个关联“数据库”，当用户在浏览器中输入一个需要登录的网址时，系统会首先自动从[Hosts文件](http://baike.baidu.com/view/493742.htm)中寻找对应的[IP地址](http://baike.baidu.com/view/3930.htm)，一旦找到，系统会立即打开对应网页，如果没有找到，则系统会再将网址提交DNS[域名解析](http://baike.baidu.com/view/30676.htm)服务器进行IP地址的解析。Windows10中，其路径位于C:\WINDOWS\system32\drivers\etc。

最后，对于关键字过滤而言，我们可以通过使用https协议来解决。https协议使用443端口，相对于http而言，在传输过程中使用了加密方式，所以防火墙无法进行关键字的检测。（需要说明的是，https传输需要先获得ssl证书，而获得证书的过程却是非加密的）。

**在进行试验的过程中，个人产生了疑惑如下：**

**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？ 按理说没有经过DNS解析，又使用的是https协议， 效果应该和替换hosts效果一样啊。而且在替换完hosts文件后在这么做就可以了，又是为什么呢？**

**遗憾的是，这个问题还没有找到答案。**

下面再来说一说IPV6 + hosts文件的方式，这种方式在几年前由于ipv6具有速度快，不计流量的特点，曾经风靡一时。但是现在谷歌官方ipv6被墙，国外又很少有用ipv6的人，导致新的IP没有发掘吗，所以已经不再有用。

不过还是想介绍一下怎么使用ipv6

首先看自己是有ipv6, 使用ipconfig命令，由于我使用的是校园网，所以可以获取ipv6

当然ipv4的用户也可以访问ipv6,可以通过在命令行中输入如下指令。

netsh   
netsh>int   
netsh interface ipv6>isatap

netsh interface ipv6> set router isatap.sjtu.edu.cn

netsh interface ipv6>set state enabled

该命令通过isatap隧道技术实现ipv4到ipv6的转换。