Windows PC 配置DNS黑名单

漏洞相关 **极速快车手** 2024-06-28 发表

组网及说明

DNS基于UDP 53号端口，诞生于1983年并沿用至今。如今DNS流量占比不足1%但是其中的攻击流量却占比90%以上。根据思科年度报告近91.3%的恶意软件被发现使用DNS作为主要手段。

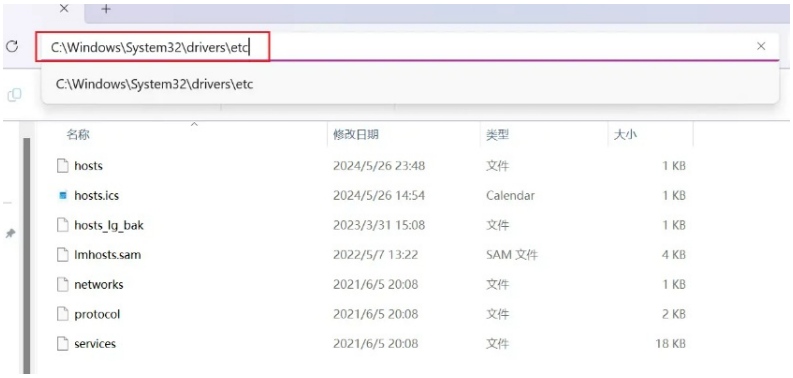
因此如果你的办公电脑被审计到软件自动访问恶意域名，就需要引起重视。

Windows PC中的防火墙通常只支持限制ip的安全策略，无法实现恶意域名拦截。
修改host文件可以实现恶意域名黑名单功能。

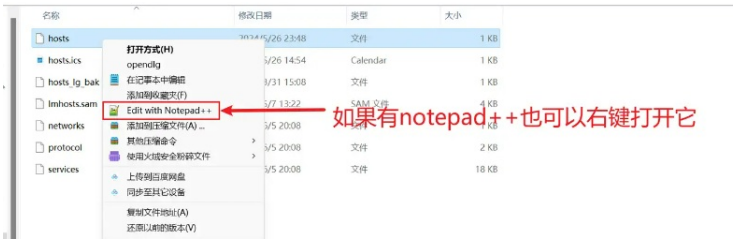
配置步骤

1. 打开windows的资源管理器(快捷键:win + E)，进入 C:\Windows\System32\drivers\etc 文件夹

(把上面这个路径复制以后，粘贴在地址栏再按回车就可以快捷进入了)



2. 我们可以看到这个文件夹里有一个叫 hosts 的文件，双击打开它



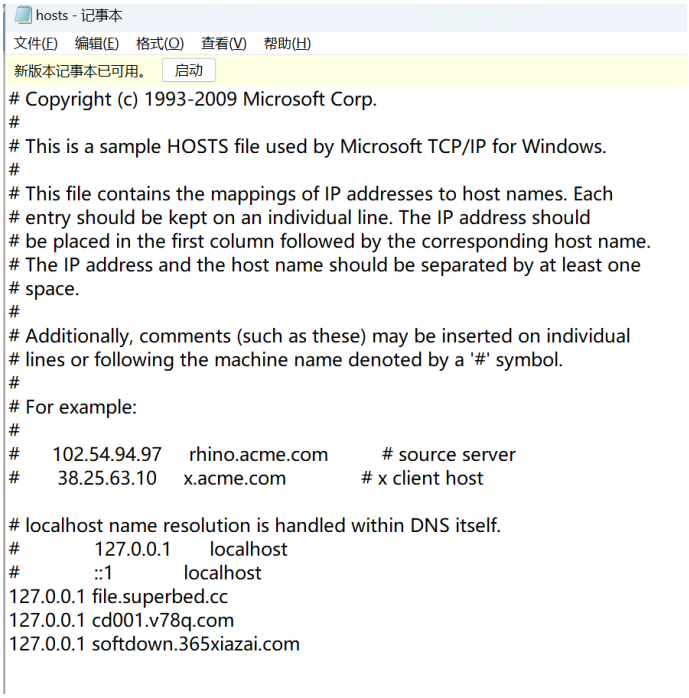
3. 打开以后，在最后一行添加

127.0.0.1 www.bilibili.com

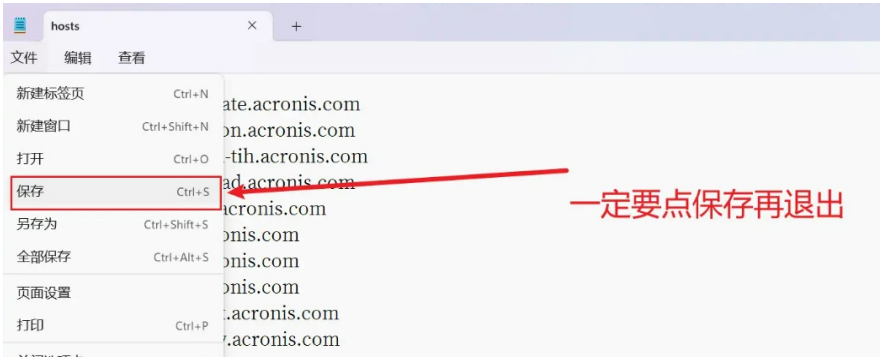
注意前面不要加空格，井号。ip地址和网址之间有一个空格

如果你是想实现访问不了其它恶意域名，请将bilibili.com改为目标恶意域名，例如softdown.365xiazai.com，这样这台电脑就无法进行百度搜索了。并且可以输入多行内容，每写完一个IP+网址以后，另起一行继续输入就行了。

例如下面这样：

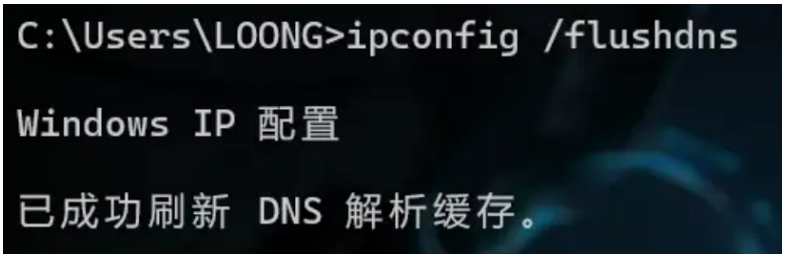


4.内容书写完以后一定要保存，或者按快捷键 *ctrl + s* 进行保存



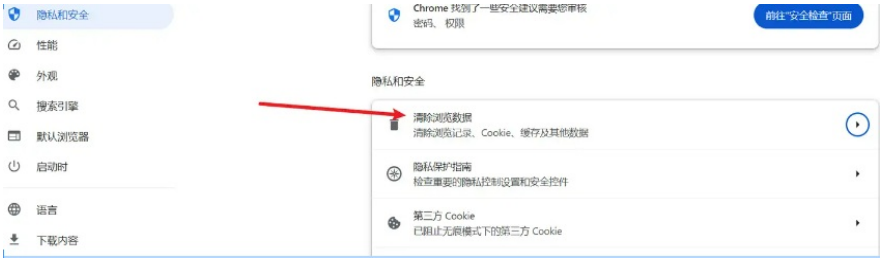
5. 然后按win + R 输入cmd代开终端

6. 在命令行里输入 `ipconfig /flushdns` 点击回车即可



好了，**现在再去访问，你就会发现无论如何也打不开了。**就算**重连网络，更换浏览器**也不行。而且因为我们的做法是修改系统文件内容，也不会被杀毒软件检测到。

当然如果还可以访问的话，可能是浏览器缓存问题，进入浏览器的设置清除一下就可以了



最后再说一下撤销的方法，那就是把刚才在 `hosts` 文件里写的内容删除就行了

配置关键点

在我们访问网站时，域名解析的优先级是： `DNS缓存 > hosts文件 > 找网关，访问DNS服务器`

假设b站的ip地址是119.84.174.66，在我们访问某域名时，正常情况下会找先DNS缓存，再找hosts里的信息，最后找路由器来获取web的ip地址。总之正常情况下获取到的肯定是正确的ip地址，但是如果将hosts文件修改为127.0.0.1对应恶意域名时在系统解析时就会定位到的ip地址为127.0.0.1，这是系统的环回地址，所以肯定无法访问到了。另外为了防止DNS缓存先人一步匹配到正确的ip地址，于是我们在cmd中删除了DNS缓存，这样就万无一失了。