

Hosts 文件域名映射劫持实验

hosts 文件是一个没有扩展名的文件，通常的路径在 C:\Windows\system32\drivers\etc\文件夹内。

该文件的作用是加快域名解析，尤其是经常访问的网站，用户可以通过在 Hosts 中配置域名和 IP 的映射关系，提高域名解析速度。由于有了映射关系，输入域名计算机就能很快解析出 IP，而不用请求网络上的 DNS 服务器。由此可见 hosts 权限要高于 DNS 服务器解析。正因为这个缘故，往往会被病毒、木马、不良程序所劫持而利用。



屏蔽网站（域名重定向）：

有很多网站不经过用户同意就将各种各样的插件安装到计算机中, 其中有些是木马或病毒。对于这些网站可以利用 Hosts 文件的权限, 把该网站的域名映射到错误的 IP 或本地计算机的 IP, 这样就不用访问不良网站了。在 WINDOWS 系

统中, 约定 127.0.0.1 为本地计算机的 IP 地址, 0.0.0.0 是错误的 IP 地址。下图是一个被劫持的 hosts 文件。



如果, 在 Hosts 中, 写入以下内容:

127.0.0.1 # 要屏蔽的网站 A

0.0.0.0 # 要屏蔽的网站 B

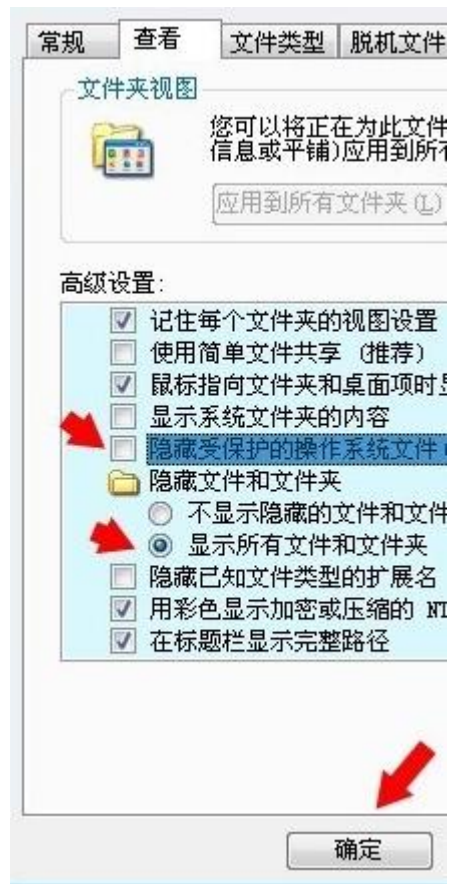
这样, 计算机解析域名 A 和 B 时, 就解析到本机 IP 或错误的 IP, 达到了屏蔽网站 A 和 B 的目的。下图是修改后的 hosts 文件 (屏蔽了不良网站)。



因为 hosts 文件是隐藏文件, 如果找不到, 可以将系统文件显示即可, 步骤是:

开始→控制面板→文件夹选项→查看→去掉【隐藏受保护的操作系统文件】

前的对勾，选中【隐藏文件和文件夹】→【显示所有文件和文件夹】→确定



不同的操作系统，可能 hosts 所在位置不一样。可以建立一个批处理文件，双击即可打开 hosts 文件，对其进行处理，这样比较便捷。步骤是：使用鼠标右键点击桌面空白处，在弹出的菜单中点选新建→文本文档

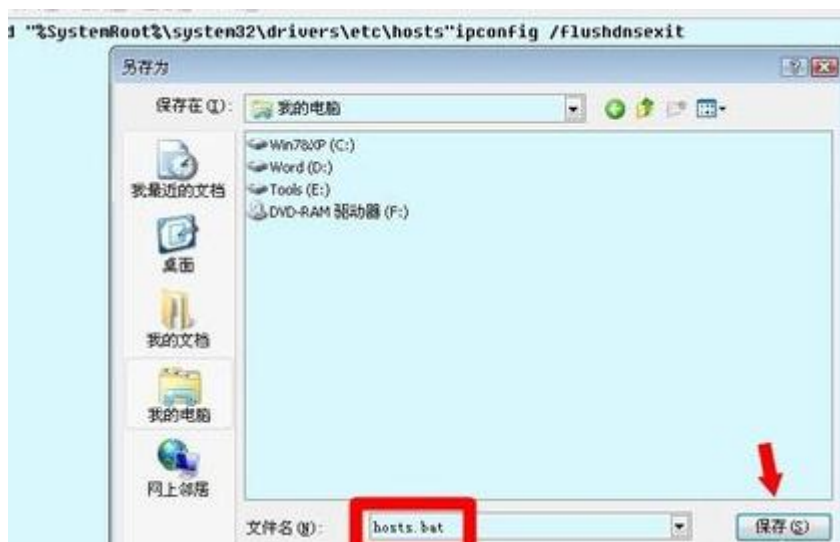


复制 (Ctrl+C) 下面这句命令, 将其黏贴 (Ctrl+V) 在新建的记事本中。

```
notepad "%SystemRoot%\system32\drivers\etc\hosts"ipconfig  
/flushdnsexit
```



文件→另存为: hosts.bat →保存



需要查看的时候, 双击这个批处理文件即可查看 (乱码是因为其中有中文)。

The screenshot shows a Windows XP desktop with a command prompt window and a Notepad window. The command prompt window has the title bar "C:\Windows\system32\cmd.exe" and contains the following text:

```
C:\MinXP\Documents and Settings\Administrator>notepad "C:\MINXP\WINDOWS\system32\drivers\etc\hosts"
ipconfig /flushdns
exit
```

The Notepad window has the title bar "hosts - 记事本" and contains the following text:

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

# copyright (c) 1993-1999 microsoft corp.
#
# this is a sample hosts file used by microsoft tcp/ip for windows.
#
# this file contains the mappings of ip addresses to host names. each
# entry should be kept on an individual line. the ip address should
# be placed in the first column followed by the corresponding host name.
# the ip address and the host name should be separated by at least one
# space.
#
# additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# for example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# 0?????0006-2007?0aD??IE?D? ?0?? / ?2?2????????[ ?]???
#127.0.0.1               localhost
#127.0.0.1               858656.com
#127.0.0.1               my123.com
#127.0.0.1               8749.com
#127.0.0.1               4199.com
#127.0.0.1               7379.com
#127.0.0.1               7055.com
```

如果 hosts 文件被劫持，可以清空文件中的所有内容，之后粘贴一句：

127.0.0.1 localhost 保存为隐藏文件即可。