# **Everything定位Webshell**

**Everything是速度最快的文件名搜索软件。其速度之快令人震惊，百G硬盘几十万个文件，可以在几秒钟之内完成索引；文件名搜索瞬间呈现结果。它小巧免费，支持中文，支持正则表达式，可以通过HTTP或FTP分享搜索结果。**

Everything搜索工具的最大优点是速度。其速度不是快，是极快；用户不是满意，而是震惊。因为Everything的索引无需逐一扫描硬盘文件，而是直接读取NTFS文件系统的USN日志。所以速度已经快到令人震惊，甚至是愤怒了：凭什么可以这么快！

“善用佳软”上有Everything的详细介绍：[http://xbeta.info/everything-search-tool.htm](http://xbeta.info/everything-search-tool.htm" \o "Everything:速度最快的文件名搜索工具" \t "http://www.freebuf.com/articles/web/_blank)

**—–分割线—–**

小菜最近闲着无事，搭建了一个blog，但因为是第一次，比较紧张，害怕被黑客入侵，所以狂补安全方面的知识，但无奈自身水平不够，而且在了解了一些安全知识之后认为如果网站被盯上了，被入侵是迟早的是，所以，我只好做被入侵之后的打算了：尽可能的查找被嵌入的webshell……

然后最近也在总结一些软件的使用经验，刚好到了Everything这款搜索神器，学着学着就想试试用Everything来辅助webshell的查找，也就有了下面的内容（这里查找的思路是通过文件的修改时间来进行判断的，因为对于一个相对稳定的网站来说，网页代码不会经常性的发生变化，所以可以通过文件的修改时间进行辅助判断）：

1.通过文件的修改日期

dateaccessed:<date>    #搜索在指定日期被访问的文件或文件夹

datecreated:<date>     #搜索在指定日期被创建的文件或文件夹

datemodified:<date>    #搜索在指定日期被修改的文件或文件夹

da:<date>           #dateaccessed:<date>的简写

dc:<date>           #datecreated:<date>的简写

dm:<date>           #datemodified:<date>的简写

其中的date的语法格式和一些常量如下：

date格式:

year

month/year or year/month depending on locale settings

day/month/year, month/day/year or year/month/day depending on locale settings

一些date的常量:

today

yesterday

tomorrow<last|past|prev|current|this|coming|next><year|month|week><last|past|prev|coming|next><x><years|months|weeks|hours|minutes|mins|seconds|secs>

january|february|march|april|may|june|july|august|september|october|november|december

jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec

sunday|monday|tuesday|wednesday|thursday|friday|saturday

sun|mon|tue|wed|thu|fri|sat

unknown

实际使用举例如下：

C:\Users\userName\Desktop datecreated:yesterday    #查找桌面上昨天修改过的文件or文件夹

C:\Users\userName\Desktop datemodified:today    #查找桌面上今天修改过的文件or文件夹

C:\Users\userName\Desktop datemodified:2014/6/15    #查找桌面上在2014/6/15这天修改过的文件or文件夹{2014/6/15这个格式和你本地的设定有关，你可以打开Everything看"Date Modified"那一列的显示格式}

C:\Users\userName\Desktop datemodified:lastweek    #查找桌面上上个星期修改过的文件or文件夹

C:\Users\userName\Desktop datemodified:january    #查找桌面上在一月份修改过的文件or文件夹

提示：最好指定一个路径来进行搜索（例如在进行webshell检测时，指定网站目录），否则速度很慢{当然了，这与个人电脑配置有关，在我的瓜机上面很慢就是了}

2.通过文件大小

使用语法介绍：

size:<size>Search for files with the specified size in bytes.

Size Syntax:

size[kb|mb|gb]

Size Constants:

empty

tiny0 KB < size <= 10 KB

small10 KB < size <= 100 KB

medium100 KB < size <= 1 MB

large1 MB < size <= 16 MB

huge16 MB < size <= 128 MB

giganticsize > 128 MB

unknown

实际举例如下：

一般的webshell文件也不大{当然了，区分大小马}，所以可以试试查找大于0KB小于10KB的文件（**size:tiny**）

查找文件大小小于50KB的文件方法（**size:<=50kb**）

当然也可以通过查找PHP文件，然后再按文件大小排序的方式来进行。

3.简洁实用的手动方式

C:\Apache\htdocs \*.php#显示了结果之后，再按照文件修改时间/大小/文件名排序，快速而且直接

C:\Apache\htdocs \*.php | \*.jpg

一般是通过指定搜索路径的方式来加快速度，可以通过多种方式的结合来达到自己的目的，这个需要根据自己的情况来定，这里就不细说了。

上面提供的只是一种思路，在Windows上也可以通过批处理脚本或PHP/Python脚本编写功能更强大的webshell查找工具（之前在Freebuf上也有过几篇很好的文章，比如：[http://www.freebuf.com/tools/8341.html](http://www.freebuf.com/tools/8341.html" \o "查找phpwebshell小工具" \t "http://www.freebuf.com/articles/web/_blank)），不过就效率，速度和直观性而言，Everything这款工具确实还是非常值得推荐的！Everything还有很多的功能值得我们去发现、去挖掘，多组合、多尝试就可以找到适合自己的方法，祝好运！

编程高手也可以自行编写脚本调用Everything的命令行来进行周期性的扫描、报告，如果写好了能给大家分享一下那就更好了(☆\_☆)/~~

————————–

在Linux上因为原生集成了很多命令行工具，速度也是非常快，所以也不用其他多余的工具了，写个shell脚本，然后放在crontab中周期性运行并把结果发送给自己，效果还是很不错的。

—–下面是从网上搜集的一些使用find/xargs/grep的命令组合查找webshell的方法—–

查找"/path/to/webroot"目录里面在10天内进行过修改的php文件（可根据需要进行微调）：

find /path/to/webroot -name "\*.php" -mtime -10

如果文件更新时间不确定，我们可以通过查找关键字的方法来确定。要想查的准确需要熟悉webshell常用的关键字，我这里列出一些常用的，其他的大家可以从网收集一些webshell，总结自己的关键字，括号里面我总结的一些关键字（eval,shell\_exec,passthru,popen,system）查找方法如下：

find /path/to/webroot -name "\*.php" |xargs grep "eval" |less

find /path/to/webroot -name "\*.php" |xargs grep "shell\_exec" |less

find /path/to/webroot -name "\*.php" |xargs grep "passthru" |less

当然你还可以导出到文件，下载下来慢慢分析：

find /home -name "\*.php"|xargs grep "fsockopen"|tee webshell\_scan.log

这里我就不一一罗列了，如果有自己总结的关键字直接替换就可以。当然并不是所有的找出的文件都是webshell，这个需要自己做一下判断，判断的方法也简单，直接从浏览器访问一下这个文件或者和自己找的一些webshell比较一下，看得多了，基本上一眼就可以判断是不是webshell文件。

因为Linux上的这个的查找方法在各种网站上都有类似的内容，没法找到原文出处，如有请告知，谢谢。