dnsenum.pl 版本:1.2.3

格式: dnsenum.pl [参数] <domain> 代指域 或者域名

[参数]:

注意: -f 是强制开启的

选项:

--dnsserver <服务器r>

一个使用此DNS服务器，NS和MX查询。

--enum 快速扫描 相当于线程数 5 -s 15 -w.

-h, --help 打印此帮助消息。

--noreverse 跳过反向查找操作。

--nocolor 禁用ansicolor输出。

--private 显示在文件domain\_ips.txt最终拯救大兵IPS。 ？？？

--subfile <file> 所有有效的子域写入这个文件的。

-t, --timeout <value> TCP和UDP超时值 默认为10

--threads <value> 将执行不同查询的线程数。

-v, --verbose 很详细：显示所有结果

谷歌搜索选项:

-p, --pages <value> 当搜索关键词时谷歌搜索页面的数量，默认为5页，必须指定搜索页数是多少

-s, --scrap <value> 他最大的子域，将搜索结果的谷歌数（默认为15）。

暴力破解:

-f, --file <file> 从这个文件读取子域进行暴力破解。

-u, --update <a|g|r|z>

更新这个软件 用-f

a (all) 使用所有结果更新。

g 更新只使用谷歌刮结果。

r 更新只使用反向查找结果。

z 更新只使用区域转移的结果。

-r, --recursion 递归穷举所有子域，子域的NS记录发现。

WHOIS NETRANGE 选项:

-d, --delay <value> Whois查询等待的最大值，该值定义随机 默认为3

-w, --whois 执行C类网络范围的WHOIS查询。

\*\*Warning\*\*:这可以产生非常大的netranges要花很多时间进行反向查找。反向查找选项:

-e, --exclude <regexp>

xclude PTR记录，从反向查找结果表达式表达式匹配，对无效的主机名有用

输出选项:

-o --output <file> 输出的XML格式. Can be imported in MagicTree (www.gremwell.com)