Version: 0.8.10

格式: dnsrecon.py <参数>

参数:

-h, --help 显示这个工具的帮助文件

-d, --domain <domain> 目标域

-r, --range <range> 用于逆向查找格式的暴力破解的IP范围 (first-last) 还是活着一个范围

-n, --name\_server <name> 域服务器使用。如果没有指定，该目标将SOA应用。

-D, --dictionary <file> 使用暴力破解对子域名和主机名破解

-f 滤出暴力破解的域，记录，解决通配符定义并保存记录时的IP地址。

-t, --type <types> 执行的枚举类型：

std 使用SOA，NS，AAAA，MX和SRV如果ns axrf不成功

rvl 反向查找一个给定的CIDR或IP范围。无间路由

brt 使用一个给定的字典的蛮力域和主机。

srv SRV记录

axfr 测试区域传输的所有的纳秒服务器。 域传输

goo 用谷歌搜索的子域和主机。 snoop 执行缓存窥探对所有NS服务器对于一个给定的域，测试所有包含域的文件，给出了D选项的文件。 -d 一起使用

tld 删除了所有的顶级域名注册域名，对IANA测试TLD。顶级域名查询 zonewalk 执行一个使用纳秒记录DNSSEC区走。

-a 标准计数执行AXFR。

-s 执行一个IPv4范围反向查找在SPF记录标准枚举。

-g 用标准枚举进行谷歌枚举。

-w 进行深WHOIS记录分析和IP反向查找区域发现谁在做这个标准的枚举。

-z 执行标准枚举DNSSEC区走。

--threads <number> 使用反向查找，查找了线程数，蛮力和SRV 记录计数。

--lifetime <number> 等待服务器响应查询的时间。

--db <file> SQLite 3文件记录在数据库

--xml <file> 把找到的结果保存成xml文件

--iw 持续的暴力破解一个域，即使发现是一个通配符记录。

-c, --csv <file> 逗号分隔值文件

-j, --json <file> JSON文件。

-v 尝试使用暴力破解模式的测试。