Usage: dnschef.py [options]:

\_ \_ \_\_

| | version 0.2 | | / \_|

\_\_| |\_ \_\_ \_\_\_ \_\_\_| |\_\_ \_\_\_| |\_

/ \_` | '\_ \/ \_\_|/ \_\_| '\_ \ / \_ \ \_|

| (\_| | | | \\_\_ \ (\_\_| | | | \_\_/ |

\\_\_,\_|\_| |\_|\_\_\_/\\_\_\_|\_| |\_|\\_\_\_|\_|

iphelix@thesprawl.org

dnschef是渗透测试人员和恶意软件的一个高度可配置的DNS代理分析师。它能够精细配置的DNS回复修改或简单地代理与真正的反应。为了利用这个工具您必须手动配置DNS服务器或毒入点DNSChef。该工具需要在特权端口上运行的根特权。

选项:

-h, --help 显示此帮助消息并退出

--fakedomains=thesprawl.org,google.com

一个逗号分隔的域名列表，这将是解决了在上面指定的假值参数.所有其他域名将被解决他们真正的价值观。

--truedomains=thesprawl.org,google.com

一个逗号分隔的域名列表，这将是解决他们的真正价值观。所有其他域名将解决到在上面指定的假值参数。

Fake DNS records::

--fakeip=192.0.2.1 IP地址使用匹配的DNS查询。如果你使用此参数没有指定域名，然后所有的查询将被欺骗。考虑使用-文件参数，如果您需要定义一个以上的IP地址。

--fakeipv6=2001:db8::1

IPv6地址使用匹配的DNS查询。如果你如果没有指定域名，使用此参数，然后所有的“AAAA”查询将被欺骗。考虑使用-如果你需要定义更多的文件参数一个IPv6地址。

--fakemail=mail.fake.com

配套使用的DNS查询MX的名字。如果你使用此参数没有指定域名，然后所有的MX查询会被欺骗。考虑使用——文件参数如果你需要定义一个以上的MX记录。

--fakealias=www.fake.com

配套使用的DNS查询CNAME名称。如果你使用此参数没有指定域名，然后所有的CNAME的查询将被欺骗。考虑使用如果您需要定义一个以上的文件，文件参数Cname记录。

--fakens=ns.fake.com

配套使用的DNS查询名称。如果你使用此参数没有指定域名，然后所有的NS的查询将被欺骗。考虑使用-文件参数如果你需要定义一个以上的记录。

--file=FILE 指定一个包含域的列表的文件（每行一对）用于DNS响应。对于例如：谷歌.com = 1.1.1.1将迫使所有的查询“谷歌.com”来解决“1.1.1.1”。IPv6地址将被自动检测到。你可以更具体的结合-文件与其他争论。然而，从文件中获得的数据将优先于别人。

可选运行时参数。:

--nameservers=8.8.8.8#53 or 2001:4860:4860::8888

一个逗号分隔的列表中选择DNS服务器使用代理的请求。域名服务器可以有IP或IP #端口格式。从一个随机选择的服务器该列表将用于代理请求时提供有多台服务器。默认情况下，该工具使用谷歌的公共DNS服务器8.8.8.8时运行IPv4模式和2001:4860:4860：：8888时运行IPv6模式。

-i 127.0.0.1 or ::1, --interface=127.0.0.1 or ::1

定义一个接口使用DNS的倾听者。通过默认情况下，该工具使用127.0.0.1 IPv4模式：：1IPv6模式。

-t, --tcp 使用TCP，UDP DNS代理而不是默认的。

-6, --ipv6 在ipv6模式。

-p 53, --port=53 端口号听DNS请求。

-q, --quiet 不显示标题。