信息收集工具与用法

作者：zgzhang
原文链接：https://ld246.com/article/1495799146843
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

whois：

介绍：whois是一个标准的互联网协议，可用于收集网络注册/注册域名/ip地址和自治系统的信息

用法：whois example.com

host：

介绍：我们可以用host指令向dns服务器查询主机的ip地址

用法：host www.example.com

dig：

介绍：用于dns查询，相比host，dig更灵活，输出更清晰，甚至可以用dig处理一个文件中所有的dn查询指令

用法：dig example.com（仅返回A记录）

dig example.com any （全部类型）

dnsenum：

介绍：收集dns数据，可收集的信息分为一下几类：

-主机ip地址

-该域的dns服务器

-该域的mx记录

-能够通过谷歌搜索其他的域名和子域名

-可用字典文件对子域名进行暴力破解，kali自带dns.txt

-可对c类网段进行whois查询并计算其网络范围

-可对网段进行反向查询

-采用多线程技术，可并发查询

用法：dnsenum example.com

dnsenum -f dns.txt example.com（暴力破解）

dnsdict6：

介绍：枚举ipv6子域名的工具

用法：dnsdict6 example.com