**kali各项工具简介：**

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | 类型 | 使用模式 | 功能 |
| **dmitry** | 信息收集 |  | whois查询/子域名收集/端口扫描 |
| **dnmap** | 信息收集 |  | 用于组建分布式nmap，dnmap\_server为服务端；dnmap\_client为客户端 |
| **ike-scan** | 信息收集 |  | 收集ipsec vpn server指纹信息 |
| **maltegoce** | 信息收集 | gui | 域名/账号等关联性收集展示 |
| **netdiscover** | 信息收集 |  | 主动发出arp包和截获arp包 |
| **nmap** | 信息收集 | cmd-line | 端口服务探测和端口漏洞扫描 |
| **p0f** | 信息收集 | cmd-line | 监听网卡收发的数据包，从数据包中读取远端机器操作系统服务版本等信息 |
| **regon-ng** | 信息收集 | shell | 模仿msf的信息侦查框架 |
| **sparta** | 暴力破解 | gui | 图形版的hydra，加了端口服务扫描功能 |
| **zenmap** | 信息收集 | gui | 图形界面版的nmap |
| **golismero** | web扫描 | cmd-line | 就是一个文本版的类似awvs的web扫描器 |
| **lynis** | 系统审计 |  | 感觉有点像360首页的“立即体验”，不过只是扫描告警不能一键修复 |
| **nikto** | web扫描 |  | web扫描器 |
| **unix-privesc-check** | 系统审计 |  | 审计系统中的关键文件权限是否有异常 |
| **bed** | 系统扫描 |  | 通过发送各种模糊数据测试多种服务的缓冲区溢出漏洞的工具 |
| **burpsuite** | web代理 |  | 常用web代理截包工具 |
| **commix** | 注入检测 |  | sqlmap检测sql注入此工具检测系统命令注入 |
| **httrack** | 网站克隆 |  | 将网站克隆到本地 |
| **owasp-zap** | web代理 | gui | owasp组织开发的工具 |
| **paros** | web扫描 | gui | 一个web爬行和漏扫工具 |
| **skipfish** | web扫描 | cmd-line | 一个全自动化的web漏洞扫描工具 |
| **sqlmap** | sql注入扫描 | cmd-line | 一个强大的sql注入扫描工具 |
| **w3af** | web扫描 | shell/gui | 一个web漏洞扫描框架 |
| **webscarab** | http代理 | gui | 更专业的网站树型结构分析工具 |
| **wpscan** | web扫描 |  | 针对wordpress的漏洞扫描工具 |
| **bbqsql** | 盲注扫描 | shell | 一个高度可配置的交互式的sql盲注工具 |
| **hexorbase** | 数据库管理 | gui | 一个支持多种数据库的客户端有多个数据库的口令破解功能 |
| **jsql** | 数据库探测 | gui | 根据url探测数据库类型/参数注入测试/探测后台页而/探测重要文件 |
| **mdb-sql** | 数据库管理 | cmd-line | 可用来连接access数据库文件（mdb）然后通过sql语句查询数据 |
| **oscaner** | 数据库猜解 | cmd-line | 用字典探查oracle数据库是否监听及猜解服务名 |
| **sidguesser** | 数据库猜解 | cmd-line | 用字典探测oracle数据库存在的sid |
| **sqllite database** | 数据库管理 | gui | sqlite数据库客户端 |
| **sqlinja** | 数据库猜解 | cmd-line | 用于猜解ms sql |
| **sqlsus** | sql注入检测 | cmd-line | 用于mysql的盲注检测 |
| **tnscmd10g** | 数据库探测 | cmd-line | 用于探测oracle是否监听及其他一些信息 |
| **cewl** | 口令文件制作 | cmd-line | 爬取给定的URL并依据限制条件截取网页中的单词生成口令集合 |
| **crunch** | 口令文件制作 | cmd-line | 依据限定的条件生成口令集合 |
| **hashcat** | hash爆破 | cmd-line | 多种hash的爆力猜解工具，速度快所耗CPU小（相对） |
| **john** | 系统口令破解 | cmd-line | 用于对系统口令文件的破解（如/etc/passwd）还原出密码明文 |
| **johnny** | 系统口令破解 | gui | john的gui版本 |
| **medusa** | 口令猜解 | cmd-line | 可对IMAP, rlogin, SSH等进行口令猜解，类似hydra |
| **ncrack** | 口令猜解 | cmd-line | 可对IMAP, rlogin, SSH等进行口令猜解，类似hydra |
| **ophcrack** | 系统口令破解 | gui | 基于彩虹表的windows口令破解工具 |
| **pyrit** | wifi破解 | cmd-line | WPA/WPA2加密的wifi的密码破解工具 |
| **rainbowcrack** | hash破解 | cmd-line | 具有彩虹表的生成、排序和使用排序好换彩虹表进行破解的功能 |
| **rcracki\_mt** | hash破解 | cmd-line | 基于彩虹表的hash破解工具，可能蚲rainbowcrack一部份 |
| **wordlist** | 口令文件 | cmd-line | 打印kali自带的一些口令文件存放的位置 |
| **aircrack-ng** | wifi破解 | cmd-line | 针对WEP、 WPA加密方式的wifi密码破解套件 |
| **chirp** | 无线电拦截 | gui | 各种无线电数据包的拦截工具（？） |
| **cowpatty** | wifi破解 | cmd-line | 基于已捕获握手包和密码字典的WPA-PSK加密的wifi密码的猜解 |
| **Fern WIFI Cracker** | wifi破解 | gui | 基于字典的WEP和WPA加密的wifi破解工具 |
| **Ghost Phiser** | AP假冒 | gui | 能发现AP并使与AP连接的设备断开连接然后假冒AP让设备重新连接 |
| **giskismet** | 可视化 | gui | Kismet输出结果的可视化工具，即较成text、html等各种格式 |
| **kismet** | AP发现 | shell | 交互式的AP发现工具，列出周围AP的各种信息 |
| [**MDK3**](http://www.360doc.com/content/15/1229/16/29791812_523958566.shtml) | AP扰乱 | cmd-line | 可向AP发送大量连接、断开请求，可向周围设备告知存在根本不存在的大量AP |
| **mfor** | IC卡破解 | cmd-line | IC卡密钥破解程序 |
| **mfterm** | IC卡破解 | shell | 交互式IC卡文件写入工具 |
| **pixiewps** | wifi破解 | cmd-line | 针对开启WPS的wifi利用WPS随机数生成中的bug来破解 |
| **reaver** | wifi破解 | cmd-line | 针对开启WPS的wifi进行暴力破解的工具 |
| **wifite** | wifi破解 | cmd-line | 较为自动化的wifi破解工具 |
| **apktool** | 安卓逆向 | cmd-line | 从apk文件中还原出xml和图版等资源文件 |
| **clang** | 编译器 | cmd-line | 类似gcc的编译器，更轻量，可编译c、c++、Objective-C |
| **clang++** | 编译器 | cmd-line | C++编译器，与clang的关系类似gcc和g++的类系 |
| **dex2jar** | 安卓逆向 | cmd-line | apktool把apk还原成了资源文件和dex，dex2jar把dex还原成jar文件（.class） |
| **edb-debug** | 动态调试 | gui | 软件逆向动态调试工具 |
| **flashm** | 反汇编 | cmd-line | .swf文件的反汇编工具可反汇编出.swf中的脚本代码 |
| **jad** | 反编译 | cmd-line | dex2jar把文件还原成了.class，jad进一步把文件还原成.java文件 |
| **javasnoop** | fuzz | gui | java程序漏洞评估工具 |
| **nasm shell** | 汇编 | shell | nasm是32位汇编编译器，这是一个nasm的shell |
| **ollydbg** | 动态调试 | gui | windows平台大名鼎鼎的动态调试工具，Linux上是通过wine运行有点水土不服 |
| **radare2** | 静态分析 | cmd-line | 类似ida的静态反汇编分析工具，功能强大，开源 |
| **armitage** | 漏洞利用 | gui | measploit的gui界面 |
| **beef** | 漏洞利用 | cmd-line | 利用msf的exp结合xss构造有攻击性的html页面，当浏览器访问即会受到攻击并获取shell |
| **metasploit** | 漏洞利用 | shell | 就是启动msfconsole咯 |
| **msf payload center** | 漏洞利用 | cmd-line | 生成包含exp的windows/android等各平台的可执行文件，木马制作利器 |
| **searchsploit** | 漏洞利用 | cmd-line | 用于搜索已从exploitdb下载到本地的漏洞利用脚本 |
| **Social-Engineering** | 漏洞利用 | shell | 一般用于生成各种插入了exp的文件，诱使目标打开而中招 |
| **termineter** | 漏洞利用 | shell | 智能电表攻击框架 |
| **bdfproxy** | 中间人攻击 |  | 处于中间人身份时可对经过的流量插入payload |
| **driftnet** | 图版嗅探 | cmd-line | 用于嗅探流量中的图版并展示到x-window上 |
| **ettercap** | 流量拦截 | gui | 听说可以截持同子网的流量，强无敌，原理是什么 |
| **hampster** | 代理 | cmd-line | 好像也是代理转发流量的 |
| **macchanger** | mac欺骗 | cmd-line | 修改本机上网时的mac地址，一用作身份隐藏，二可用来绕过wifi mac黑名单 |
| **mitmproxy** | 代理 | cmd-line | 好像也是代理转发流量的 |
| **netsniff-ng** | 流量捕获 | cmd-line | 高性能的流量捕获套件，可能大流量时的捕获效果比较稳定 |
| **responder** | 主机嗅探 | cmd-line | 被动嗅探与所在主机交互的主机的操作系统版本等信息 |
| **wireshark** | 流量捕获 | gui | 拦截经过指定网卡的所有流量 |
| **backdoor** |  |  |  |
| **exe2hex** | 编码转换 | cmd | 顾名思义就是把exe文件转成十六进制文件 |
| **Intersect** | 脚本生成 | shell | 感觉是SQL 有攻击性Intersect语句的生成工具 |
| **mimikatz** | 密码提取 | cmd-line | 用于从windows内存中提取密码 |
| **nishang** | 后渗透 | cmd-line | 基于powershell的后渗透攻击工具 |
| **PowerSploit** | 后渗透 | cmd-line | 也是一个基于powershell的后渗透攻击工具 |
| **proxychains** | 多重代理 | cmd-line | 好像用来配置多种代理的 |
| **weevely** | webshell | shell | webshell连接工具不过好像要用自己生成的小马 |
| **autopsy** | 网页分析 | web | 启动一个服务通过浏览器访问使用，感觉是分析网页各种元素的不是很懂 |
| **binwalk** | 文件识别 | cmd-line | 用于分析一个文件中是否其实有多个文件 |
| **bulk\_extractor** | 要素提取 | cmd-line | 扫描给定的目录或文件，如果发现一些如电话号码网址等关键的信息则输出到文件 |
| **chkrootkit** | 系统检查 | cmd-line | 扫描本机，查看本机是否存在受rootkit影响的地方 |
| **foremost** | 文件恢复 | cmd-line | 文件恢复工具，用于被删除的文件的恢复，就是360等的那个文件恢复功能 |
| **galleta** | cookie文件 | cmd-line | 用于分析IE的cookie文件输出其中的有用信息 |
| **hashdeep** | hash计算 | cmd-line | 用于计算文件hash值，支持多种散列算法 |
| **volafox** | 内存分析 | cmd-line | 针对Mac OS X的内存分析工具，可从其内存镜像中读取进程列表等各种主机信息 |
| [**volatility**](http://www.jianshu.com/p/5f13ee20f5b0) | 内存分析 | cmd-line | volafox的扩展，支持Mac OS X/Linux/Windows |
| **casefile** | 报告编写 | gui | 一个画图工具，packet tracer用来画网络拓扑，这用来画场景拓扑 |
| **cutycapt** | 网页截屏 | cmd-line | 一个基于WebKit内核的网页截图工具，就是指定一个url它就能用解析url并把url界面截下来 |
| **dradis** | 报告生成 | web | 可解析burpsuite/nmap等生成的扫描文件，并可将扫描结果转存为pdf或html |
| **faraday IDE** | 报告管理 | gui |  |
| **keepnote** | 笔记本 | gui | 较之记事本，可建文件夹，支持富文本，可导出为其他格式 |
| **magictree** | 报告管理 | gui |  |
| **pipal** | 词频统计 | cmd-line | 说词频统计并不是很准确，文命令可分析统计给定文件中的词语的“[各种最](http://www.freebuf.com/sectool/49592.html)” |
| **recordmydesktop** | 屏幕录制 | cmd-line | 屏幕录制，输出.ogv格式视频 |
| **maltegoce** | 关系分析 | gui | 通过网络搜索，获取某个IP或邮箱与其他IP或邮箱的拓扑关系 |