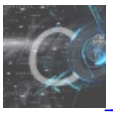
红队渗透测试 | 攻防 | 学习 | 工具 | 分析 | 研究资料汇总

原创

CKCsec 于 2022-01-07 15:53:07 发布 3772 收藏 69

分类专栏： 安全学习笔记 文章标签： 渗透测试 web安全

本文链接：https://blog.csdn.net/qq_46717339/article/details/122366277



红队渗透测试 | 攻防 | 学习 | 工具 | 分析 | 研究资料汇总

关注公众号 **CKCsec安全团队** 回复 **0107** 获取PDF 版下载链接

目录导航

- MS 与 Office 漏洞收集
- Kali 环境下拓展插件
- Nessus 相关工具拓展插件
- Awvs 相关工具拓展插件
- Burpsuit 相关工具拓展插件
- Sqlmap 相关工具拓展插件
- Nmap 相关工具拓展插件
- Metasploit 相关工具拓展插件
- CobaltStrike 相关工具拓展插件
- Empire 相关工具拓展插件
- 信息搜集
- 敏感信息泄露发现
- 威胁情报分析
- 托管云安全
- 目录路径发现
- 本地文件包含漏洞
- 安全测试与扫描器框架
- 运维安全服务与资产管理
- 上传漏洞利用
- 端口发现服务指纹识别
- 数据库扫描与爆破
- XSS 跨站脚本检测利用
- 弱口令扫描爆破
- 密码破解还原
- 网站管理与 Webshell
- 内网拓展后渗透
- 远程控制 C2 服务器
- 端口转发与代理工具
- Cross 超越边界 NPV
- 横向移动与密码 Hash 窃取
- Linux 提权相关
- Windows 提权相关
- 权限绕过
- 沙盒逃逸
- 后门免杀代码混淆
- 文件捆绑
- 社工相关
- 钓鱼框架邮件伪造

- 中间人攻击流量劫持
- 协议解析流量还原分析
- 无线网络 WIFI 中间人攻击
- 无线网络 WIFI 防御
- 无线网络 WIFI 审计测试
- 数据取回隐秘传输
- 硬件安全
- IoT 安全
- 摄像头安全
- 路由安全
- 物联网安全
- Fuzz 模糊测试漏洞挖掘
- 安全防护
- 代码审计应用测试
- 大数据平台安全
- 蜜罐安全
- Web 蜜罐内网监测
- 摄像头蜜罐
- 工控蜜罐
- 逆向相关
- CTF 相关
- 计算机与移动设备取证调查
- 移动安全
- 防火墙规则、Waf、CDN 相关
- 入侵检测
- 恶意文件测与样本分析
- 恶意文件检测之 Webshell 查杀扫描
- 压力测试与 DDOS 相关
- 匿名信息保护洋葱路由 TorBrowser
- 爬虫相关
- 在线自服务与工具
- 在线办公套件
- 隐私匿名加密
- 在线资源

相关资源列表

```
https://mitre-attack.github.io/ mitre 科技机构对攻击技术的总结 wiki
https://huntingday.github.io MITRE | ATT&CK 中文站[https://www.ddosi.org/att/]
https://arxiv.org 康奈尔大学（Cornell University）开放文档
http://www.owasp.org.cn/owasp-project/owasp-things OWASP 项目
http://www.irongeek.com/i.php?page=security/hackingillustrated 国内外安全大会相关视频与文档
https://github.com/knownsec/KCon KCon 大会文章 PPT
https://github.com/SecWiki/sec-chart 各种相关安全思维导图集合
https://github.com/knownsec/RD_Checklist 知道创宇技能列表
https://github.com/ChrisLinn/greyhame-2017 灰袍技能书 2017 版本
https://github.com/Hack-with-Github/Awesome-Hacking GitHub 万星推荐：黑客成长技术清单
https://github.com/k4m4/movies-for-hackers 安全相关电影
https://github.com/jaredthecoder/awesome-vehicle-security 一个用于了解车辆安全和汽车黑客的资源
```

清单

```
https://www.jianshu.com/p/852e0fbe2f4c 安全产品厂商分类
https://www.reddit.com/r/Python/comments/a81mg3/the_entire_mit_intro_computer_science_class_using/ 麻省理工机器学习视频
https://github.com/fxsjy/jieba py，结巴中文分词
https://github.com/thunlp/THULAC-Python py，清华中文分词
https://github.com/lancopku/PKUSeg-python py3，北大中文分词
https://github.com/fengdu78/Coursera-ML-AndrewNg-Notes 吴恩达机器学习 python 笔记
https://paperswithcode.com/sota 机器学习具体项目、演示、代码
https://github.com/duoergun0729/nlp 一本开源的 NLP（神经语言程序学）入门书籍
https://www.freebuf.com/articles/web/195304.html 一句话木马的套路
```

攻防测试手册

```
https://micropoor.blogspot.com/2019/01/php8.html PHP 安全新闻早 8 点课程系列高持续渗透-Microporor
https://github.com/Micropoor/Micro8 Microporor 高级攻防 100 课
https://github.com/maskhed/Papers 包含 100 课等经典攻防教材、安全知识
https://github.com/infosecn1nja/AD-Attack-Defense 红蓝方攻防手册
https://github.com/yeyintminthuhtut/Awesome-Red-Teaming 优秀红队资源列表
https://github.com/foobarto/redteam-notebook 红队标准渗透测试流程+常用命令
https://github.com/tom0li/collection-document 文章收集：安全部、SDL、src、渗透测试、漏洞利用
https://github.com/kbandla/APTnotes 各种公开的文件和相关的 APT 笔记，还有软件样本
https://wizardforcel.gitbooks.io/web-hacking-101/content Web Hacking 101 中文版
https://techvomit.net/web-application-penetration-testing-notes/ web 渗透测试笔记
https://github.com/qazbnm456/awesome-web-security Web 安全资料和资源列表
http://pentestmonkey.net/category/cheat-sheet 渗透测试常见条目
https://github.com/demonsec666/Security-Toolkit 渗透攻击链中常用工具及使用场景
https://github.com/Kinimiwar/Penetration-Testing 渗透测试方向优秀资源收集
https://github.com/jshaw87/Cheatsheets 渗透测试/安全秘籍/笔记
```

内网安全文档

```
https://attack.mitre.org/wiki/Lateral_Movement mitre 机构对横向移动的总结
https://payloads.online/archivers/2018-11-30/1 彻底理解 Windows 认证 - 议题解读
https://github.com/klionsec/klionsec.github.io 内网大牛的学习历程
https://github.com/l3m0n/pentest_study 从零开始内网渗透学习
https://github.com/Ridter/Intranet_Penetration_Tips 内网渗透 TIPS
```

学习手册相关资源

```
https://github.com/HarmJ0y/CheatSheets 多个项目的速查手册（Beacon / Cobalt Strike，PowerView，PowerUp，Empire 和 PowerSploit）
https://wizardforcel.gitbooks.io/kali-linux-web-pentest-cookbook/content/ Kali Linux Web 渗透测试秘籍 中文版
https://github.com/louchaooo/kali-tools-zh kali 下工具使用介绍手册
https://www.offensive-security.com/metasploit-unleashed/ kali 出的 metasploit 指导笔记
http://www.hackingarticles.in/comprehensive-guide-on-hydra-a-brute-forcing-tool/ hydra 使用手册
https://www.gitbook.com/book/t0data/burpsuite/details burpsuite 实战指南
https://zhuanlan.zhihu.com/p/26618074 Nmap 扩展脚本使用方法
https://somdev.me/21-things-xss/ XSS 的 21 个扩展用途
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/ sql 注入 sheet 表
https://sqlwiki.netspi.com/ 你要的 sql 注入知识点都能找到
https://github.com/kevins1022/SQLInjectionWiki 一个专注于聚合和记录各种 SQL 注入方法的 wiki
https://github.com/hardenedlinux/linux-exploit-development-tutorial Linux exploit 开发入门
https://wizardforcel.gitbooks.io/asani/content 浅入浅出 Android 安全 中文版
https://wizardforcel.gitbooks.io/lpad/content Android 渗透测试学习手册 中文版
https://github.com/writeups/ios ios 漏洞 writeup 笔记
http://blog.safebuff.com/2016/07/03/SSRF-Tips/ ssrf 漏洞利用手册
```

Checklist 和基础安全知识

```
https://book.yunzhan365.com/umta/rtnp/mobile/index.html 网络安全科普小册子
http://sec.cuc.edu.cn/huangwei/textbook/ns/ 网络安全电子版教材。中传信安课程网站
https://mitre.github.io/attack-navigator/enterprise/ mitre 机构 att&ck 入侵检测条目
https://github.com/danielmiessler/SecLists 表类型包括用户名，密码，URL，敏感数据模式，模糊测试负载，Web shell 等
https://github.com/GitGuardian/APISecurityBestPractices api 接口测试 checklist
https://github.com/ym2011/SecurityManagement 分享在建设安全管理体系、ISO27001、等级保护、安全评审过程中的点点滴滴
https://mp.weixin.qq.com/s/O36e0gl4cs0ErQPsb5L68Q 区块链，以太坊智能合约审计 CheckList
https://github.com/slowmist/eos-bp-nodes-security-checklist 区块链，EOS bp nodes security checklist（EOS 超级节点安全执行指南）
https://xz.aliyun.com/t/2089 金融科技 SDL 安全设计 checklist
https://github.com/juliocesarfort/public-pentesting-reports 由几家咨询公司和学术安全组织发布的公共渗透测试报告的列表。
http://www.freebuf.com/articles/network/169632.html 开源软件创建 SOC 的一份清单
https://github.com/0xRadi/OWASP-Web-Checklist owasp 网站检查条目
https://www.securitypaper.org/ SDL 开发安全生命周期管理
https://github.com/Jsitech/JShielder linux 下服务器一键加固脚本
https://github.com/wstart/DB_BaseLine 数据库基线检查工具
```

产品设计文档

```
https://www.freebuf.com/sectool/135032.html 构建一个高交互型的难以发现的蜜罐
https://bloodzer0.github.io/ossa/ 利用开源文件进行开源安全架构.主机、扫描器、端口、日志、防护设备等
https://github.com/dvf/blockchain 用 Python 从零开始创建区块链
https://github.com/crazywa1ker/DarthSidious-Chinese 从 0 开始你的域渗透之旅，DarthSidious 中文版
https://paper.seebug.org/772/ 如何使用 KittyFuzzer 结合 ISF 中的工控协议组件对工控协议进行 Fuzz
```

学习靶场

```
https://www.blackmoreops.com/2018/11/06/124-legal-hacking-websites-to-practice-and-learn/ 124 个合法的可以练习 Hacking 技术的网站
https://www.zhihu.com/question/267204109 学 web 安全去哪里找各种各样的靶场？
https://www.vulnhub.com 许多 ctf 靶机汇总
https://www.wechall.net 世界知名 ctf 汇总交流网站
https://www.xssgame.com 谷歌 XSS 挑战
http://xss.tv 在线靶场挑战
https://www.hackthebox.eu 在线靶场挑战
https://www.root-me.org 在线靶场挑战
http://www.itsecgames.com bWAPP，包含 100 多种漏洞环境
https://github.com/c0ny1/vulstudy 多种漏洞复现系统的 docker 汇总
https://github.com/bkimminich/juice-shop 常见 web 安全实验靶场市场
https://github.com/ethicalhack3r/DVWA web 安全实验靶场
https://www.freebuf.com/articles/web/123779.html 新手指南：DVWA-1.9 全级别教程
https://github.com/78778443/permeate php，常见漏洞靶场
https://github.com/gh0stkey/DoraBox php,常见漏洞靶场
https://github.com/stamparm/DSVW py2,常见漏洞靶场
https://github.com/amolnaik4/bodhi py,常见漏洞靶场
https://github.com/Safflower/Solve-Me php，韩国一个偏代码审计的 ctf 靶场源码
https://github.com/WebGoat/WebGoat 一键 jar 包，web 安全实验靶场
https://github.com/Audi-1/sqli-labs 基于 SQLite 的 sql 注入学习靶场
https://github.com/lcamry/sqli-labs 通过 sqli-labs 演示 mysql 相关的注入手法
https://github.com/c0ny1/upload-labs 一个帮你总结所有类型的上传漏洞的靶场
https://github.com/LandGrey/upload-labs-writeup upload-labs 指导手册
https://github.com/Go0s/LFIboomCTF 本地文件包含漏洞&&PHP 利用协议&&实践源码
https://in.security/lin-security-practise-your-linux-privilege-escalation-foo/ 一个虚拟机文件用于 linux 提权练习
https://github.com/OWASP/igoat 适用于 ios 应用程序测试和安全性的学习工具
https://github.com/prateek147/DVIA-v2 适用于 ios 应用程序测试和安全性的学习工具
https://github.com/rapid7/metasploitable3 metasploit 练习系统
https://github.com/rapid7/metasploit-vulnerability-emulator 基于 perl 的 metasploit 模拟环境，练习操作
https://github.com/chryzsh/DarthSidious AD 域环境的搭建、渗透、防护
https://github.com/c0ny1/xxe-lab 一个包含 php,java,python,C#等各种语言版本的 XXE 漏洞 Demo
```

漏洞复现

```
https://github.com/vulhub/vulhub Vulhub 是一个面向大众的开源漏洞靶场，无需 docker 知识，执行两条命令即可编译、运行一个完整的漏洞靶场镜像
https://github.com/Medicean/VulApps 收集各种漏洞环境，为方便使用，统一采用 Dockerfile 形式。同时也收集了安全工具环境。
https://github.com/bingohuang/docker-labs 制作在线 docker 平台
```

开源漏洞库

```
https://wooyun.kieran.top/#!/ 2016 年之前，乌云 Drops 文章，公开漏洞详情文章
https://wooyun.js.org/ 2016 年之前，乌云 Drops 文章，公开漏洞详情文章
https://dvpnet.io/list/index/state/3 公开漏洞详情文章
https://sec.ly.com/bugs 同程安全公开漏洞详情文章
http://ics.cnvd.org.cn 中国国家工控漏洞库
https://ics-cert.us-cert.gov/advisories 美国国家工控漏洞库
http://www.nsfocus.net/index.php?act=sec_bug 绿盟漏洞库，含工控
http://ivd.winicssec.com/ 威努特工控漏洞库
http://cve.scap.org.cn/view/ics CVE 中文工控漏洞库
https://cve.mitre.org/cve/search_cve_list.html 美国 MITRE 公司负责维护的 CVE 漏洞库
https://www.exploit-db.com 美国 Offensive Security 的漏洞库
https://nvd.nist.gov/vuln/search 美国国家信息安全漏洞库
```

工具包集合

http://www.4hou.com/web/11241.html 史上最全攻击模拟工具盘点
https://github.com/infosecn1nja/Red-Teaming-Toolkit 信息收集、攻击尝试获得权限、持久性控制、权限提升、网络信息收集、横向移动、数据分析（在这个基础上再做持久化控制）、清理痕迹
https://github.com/toolswatch/blackhat-arsenal-tools 黑帽大会工具集
https://www.cnblogs.com/k8gege K8 哥哥工具包集合。解压密码 Kk8team,Kk8gege
https://github.com/n00py/ReadingList/blob/master/gunsafe.txt 安全工具集
https://github.com/Ridter/Pentest 安全工具集
https://github.com/redcanaryco/atomic-red-team win、linux、mac 等多方面 apt 利用手段、技术与工具集
https://github.com/Cooolis/Cooolis.github.io Cooolis 是一个操作系统命令技巧备忘录，https://cooolis.payloads.online
https://github.com/LOLBAS-Project/LOLBAS 常见的渗透测试利用的脚本与二进制文件集合
https://www.owasp.org/index.php/File:CSRFTester-1.0.zip csrf 验证工具
https://github.com/ufrisk/MemProcFS 以访问文件系统的方式访问物理内存，可读写，有易于使用的接口．当前支持 Windows
https://github.com/vletoux/SpoolerScanner 检测 Windows 远程打印机服务是否开启的工具
https://github.com/sirpsycho/firecall 直接向 CiscoASA 防火墙发送命令，无需登录防火墙后再做修改
https://github.com/jboss-javassist/javassist 能够操作字节码框架，通过它我们能很轻易的修改 class 代码文件
https://github.com/ConsenSys/mythril-classic 用于以太坊智能协议的安全分析工具
https://github.com/a13xp0p0v/kconfig-hardened-check 用于检查 Linux 内核配置中的安全加固选项的脚本
https://github.com/lionsoul2014/ip2region ip 地址定位库，支持 python3 等多接口。类比 geoip
https://github.com/m101/hsploit 基于 rust 的 HEVD 漏洞利用程序
https://github.com/ticarpi/jwt_tool 针对 json web token 的检测
https://github.com/clr2of8/DPAT 域密码配置审计
https://github.com/chenjj/CORScanner 域解析漏洞，跨域扫描器
https://github.com/dienuet/crossdomain 域解析漏洞，跨域扫描器
https://github.com/sfan5/fi6s ipv6 端口快速扫描器
https://github.com/lavalamp-/ipv666 go,ipv6 地址枚举扫描
https://github.com/commixproject/commix 命令注入漏洞扫描
https://github.com/Graph-X/davscan DAVScan 是一款快速轻便的 webdav 扫描仪，旨在发现 DAV 启用的 Web 服务器上的隐藏文件和文件夹
https://github.com/jcesarstef/dotdotslash 目录遍历漏洞测试
https://github.com/P3GLEG/WhaleTail 根据 docker 镜像生成成 dockerfile
https://github.com/cr0hn/dockerscan docker 扫描工具
https://github.com/utiso/dorkbot 通过定制化的谷歌搜索引擎进行漏洞页面搜寻及扫描
https://github.com/NullArray/DorkNet 基于搜索引擎的漏洞网页搜寻
https://github.com/panda-re/lava 大规模向程序中植入恶意程序
https://github.com/woj-ciech/Danger-zone 关联域名、IP 和电子邮件地址之间的数据并将其可视化输出
https://github.com/securemode/DefenderKeys 枚举出被 Windows Defender 排除扫描的配置
https://github.com/D4Vinci/PasteJacker 剪贴板劫持利用工具
https://github.com/JusticeRage/freedomfighting 日志清理、文件共享、反向 shell、简单爬虫工具包
https://github.com/gh0stkey/PoCBox 漏洞测试验证辅助平台，SONP 劫持、CORS、Flash 跨域资源读取、Google Hack 语法生成、URL 测试字典生成、JavaScript URL 跳转、302 URL 跳转
https://github.com/jakubroztocil/httpie http 调试工具，类似 curl，功能更完善
https://www.getpostman.com/ http 调试工具，带界面

漏洞收集与 Exp、Poc 利用

https://github.com/Lcys/Python_PoC python3 的 poc、exp 快速编写模板，有众多模范版本
https://github.com/raminfp/linux_exploit_development linux 漏洞利用开发手册
https://github.com/mudongliang/LinuxFlaw 包含 linux 下软件漏洞列表
https://github.com/coffeehb/Some-PoC-oR-ExP 各种漏洞 poc、Exp 的收集或编写
https://github.com/userlandkernel/plataoplomo Sem Voigtländer 公开其发现的 iOS 中各种漏洞，包括（Writeup/POC/Exploit）
https://github.com/coffeehb/Some-PoC-oR-ExP/blob/master/check_icmp_dos.py CVE-2018-4407，macos/ios 缓冲区溢出可导致系统崩溃
https://github.com/vulnersCom/getsploit py2,仿照 searchsploit 通过各种数据库的官方接口进行 payload 的查找
https://github.com/SecWiki/CMS-Hunter CMS 漏洞测试用例集合
https://github.com/Mr5m1th/0day 各种开源 CMS 各种版本的漏洞以及 EXP
https://github.com/w1109790800/penetration CMS 新老版本 exp 与系统漏洞搜集表
https://github.com/blacknbunny/libSSH-Authentication-Bypass CVE-2018-10933，libssh 服务端身份验证绕过
https://github.com/leapsecurity/libssh-scanner CVE-2018-10933，libssh 服务端身份验证绕过
https://github.com/anbai-inc/CVE-2018-4878 Adobe Flash Exploit 生成 payload
https://github.com/RetireJS/grunt-retire 扫描 js 扩展库的常见漏洞
https://github.com/coffeehb/SSTIF 服务器端模板注入漏洞的半自动化工具
https://github.com/tijme/angularjs-csti-scanner 探测客户端 AngularJS 模板注入漏洞工具
https://github.com/blackye/Jenkins Jenkins 漏洞探测、用户抓取爆破
https://github.com/epinna/tplmap 服务器端模板注入漏洞检测与利用工具
https://github.com/irsdl/IIS-ShortName-Scanner Java,IIS 短文件名暴力枚举漏洞利用工具
https://github.com/lijiejie/IIS_shortname_Scanner py2,IIS 短文件名漏洞扫描
https://github.com/rudSarkar/crlf-injector CRLF 注入漏洞批量扫描
https://github.com/hahwul/a2sv SSL 漏洞扫描，例如心脏滴血漏洞等
https://github.com/jagracey/Regex-DoS RegEx 拒绝服务扫描器
https://github.com/Bo0oM/PHP_imap_open_exploit 利用 imap_open 绕过 php exec 函数禁用
https://www.anquanke.com/post/id/106488 利用 mysql 服务端恶意配置读取客户端文件，（如何利用 MySQL LOCAL INFILE 读取客户端文件，Read MySQL Client’s File，【技术分享】从 MySQL 出发的反击之路）
https://www.waitalone.cn/awvs-poc.html CVE-2015-4027，AWVS10 命令执行漏洞
http://an7isec.blogspot.com/2014/04/pown-noobs-acunetix-0day.html Pwn the n00bs – Acunetix 0day，awvs8 命令执行漏洞
https://github.com/numpy/numpy/issues/12759 科学计算框架 numpy 命令执行 RCE 漏洞
https://github.com/petercunha/Jenkins-PreAuth-RCE-PoC jenkins 远程命令执行
https://github.com/WyAtu/CVE-2018-20250 WinRar 执行漏洞加使用介绍

物联网路由工控漏洞收集

https://github.com/yassineaboukir/CVE-2018-0296 测试思科 ASA 路径穿越漏洞，可获取系统详细信息
https://github.com/seclab-ucr/tcp_exploit 利用 tcp 漏洞使无线路由器产生隐私泄露
https://github.com/ezelf/CVE-2018-9995_dvr_credentials CVE-2018-9995 摄像头路由，Get DVR Credentials

Java 反序列化漏洞收集

https://github.com/brianwrf/hackUtils java 反序列化利用
https://github.com/GoSecure/break-fast-serial 借助 DNS 解析来检测 Java 反序列化漏洞工具
https://github.com/s1kr10s/Apache-Struts-v3 Apache-Struts 漏洞利用工具
https://github.com/iBearcat/S2-057 struts2 CVE-2018-11776 漏洞检测工具
https://github.com/Ivan1ee/struts2-057-exp struts2-057 利用脚本
https://github.com/theLSA/s2sniper struts2 漏洞的检测工具
https://github.com/Lucifer1993/struts-scan 批量检测 struts 命令执行漏洞
https://github.com/lijiejie/struts2_045_scan Struts2-045 漏洞批量扫描工具
https://github.com/riusksk/StrutScan 基于 perl 的 strut2 的历史漏洞扫描
https://github.com/Coalfire-Research/java-deserialization-exploits java 反序列化漏洞收集
https://github.com/quentinhardy/jndiat weblogic 漏洞利用工具
https://github.com/jas502n/CVE-2018-3191 Weblogic CVE-2018-3191 远程代码命令执行
https://github.com/pyn3rd/CVE-2018-3245 weblogic cve-2018-2893 与 cve-2018-3245 远程代码命令执行
https://github.com/NickstaDB/BaRMIe 用于 Java Remote Method Invocation 服务的工具/rmi 的枚举与远程命令执行
https://github.com/joaomatosf/jexboss JBoss 和其他 java 序列化漏洞验证和开发工具
https://github.com/frohoff/ysoserial java 反序列化利用工具

版本管理平台漏洞收集

```
https://github.com/shengqi158/svnhack .svn 文件夹泄漏利用工具
https://www.waitalone.cn/seay-svn-poc-donw-20140505.html Seay-Svn 源代码泄露漏洞利用工具，2014-05-05 版
https://github.com/BugScanTeam/GitHack .git 文件利用工具，lijiejie 改进版
https://github.com/lijiejie/GitHack .git 文件利用工具
```

MS 与 Office 漏洞收集

```
https://github.com/Lz1y/CVE-2017-8759 .NET Framework 换行符漏洞，CVE-2017-8759 完美复现（另附加 hta+powershell 弹框闪烁解决方案）https://www.freebuf.com/vuls/147793.html
https://github.com/WyAtu/CVE-2018-8581 Exchange 使用完成添加收信规则的操作进行横向渗透和提权漏洞
https://github.com/dafthack/MailSniper PS,用于在 Microsoft Exchange 环境搜索电子邮件查找特定邮件（密码、网络架构信息等）
https://github.com/sensepost/ruler GO,通过 MAPI / HTTP 或 RPC / HTTP 协议远程与 Exchange 服务器进行交互,通过客户端 Outlook 功能远程获取 shell
https://github.com/3gstudent/Smbtouch-Scanner 扫描内网永恒之蓝 ETERNAL445SMB 系列漏洞
https://github.com/smgorelik/Windows-RCE-exploits windows 命令执行 RCE 漏洞 POC 样本，分为 web 与文件两种形式
https://github.com/3gstudent/CVE-2017-8464-EXP CVE-2017-8464，win 快捷方式远程执行漏洞
https://github.com/Lz1y/CVE-2018-8420 Windows 的 msxml 解析器漏洞可以通过 ie 或 vbs 执行后门
https://www.anquanke.com/post/id/163000 利用 Excel 4.0 宏躲避杀软检测的攻击技术分析
https://github.com/BuffaloWill/oxml_xxe XXE 漏洞利用
https://thief.one/2017/06/20/1/ 浅谈 XXE 漏洞攻击与防御
https://github.com/thom-s/docx-embeddedhtml-injection word2016，滥用 Word 联机视频特征执行恶意代码 poc
https://blog.cymulate.com/abusing-microsoft-office-online-video word2016，滥用 Word 联机视频特征执行恶意代码介绍
https://github.com/0xdeadbeefJERKY/Office-DDE-Payloads 无需开启宏即可在 word 文档中利用 DDE 执行命令
http://www.freebuf.com/articles/terminal/150285.html 无需开启宏即可在 word 文档中利用 DDE 执行命令利用
https://github.com/Ridter/CVE-2017-11882 利用 word 文档 RTF 获取 shell，https://evi1cg.me/archives/CVE_2017_11882_exp.html
https://github.com/Lz1y/CVE-2017-8759 利用 word 文档 hta 获取 shell，http://www.freebuf.com/vuls/147793.html
https://fuping.site/2017/04/18/CVE-2017-0199 漏洞复现过程 WORD RTF 文档，配合 msf 利用
https://github.com/tezukanice/Office8570 利用 ppsx 幻灯片远程命令执行，https://github.com/rxwx/CVE-2017-8570
https://github.com/0x09AL/CVE-2018-8174-msf 目前支持的版本是 32 位 IE 浏览器和 32 位 office。网页访问上线，浏览器关闭，shell 依然存活，http://www.freebuf.com/vuls/173727.html
http://www.4hou.com/technology/9405.html 在 Office 文档的属性中隐藏攻击载荷
https://evi1cg.me/archives/Create_PPSX.html 构造 PPSX 钓鱼文件
https://github.com/enigma0x3/Generate-Macro PowerShell 脚本，生成含有恶意宏的 Microsoft Office 文档
https://github.com/mwrlabs/wePWNise 生成独立于体系结构的 VBA 代码，用于 Office 文档或模板，并自动绕过应用程序控制
https://github.com/curi0usJack/luckystrike 基于 ps，用于创建恶意的 Office 宏文档
https://github.com/sevagas/macro_pack MS Office 文档、VBS 格式、快捷方式 payload 捆绑
https://github.com/khr0x40sh/MacroShop 一组通过 Office 宏传递有效载荷的脚本
```

Kali 环境下拓展插件

```
https://github.com/secforce/sparta py，图形化应用程序联动 Nmap、Nikto、Hydra 等工具
https://github.com/Manisso/fsociety linux 下类似于 kali 的工具包一键安装工具
https://github.com/LionSec/katoolin 使用 linux 服务器自动安装 kali 工具包
https://github.com/skavngr/rapidscan py2，simple，联动 kali 下工具，漏洞扫描工具
https://github.com/koenbuyens/kalirouter 将 kali 设置为一个路由流量分析系统
```

Nessus 相关工具拓展插件

```
https://www.tenable.com/downloads/nessus
https://github.com/se55i0n/Awvs_Nessus_Scanner_API 扫描器 Awvs 11 和 Nessus 7 Api 利用脚本
https://github.com/DanMcInerney/msf-autoshell 配合 nessus 扫描结果进行 msf 攻击
https://github.com/MooseDojo/apt2 联动 nmap、nessus 等工具进行安全测试
```

Awvs 相关工具拓展插件

```
https://www.52pojie.cn/thread-214819-1-1.html awvs10.5 开发框架破解版
https://github.com/fnmsd/awvs_script_decode awvs10.5 规则 scripts 解密版，SDK，开发手册
https://github.com/NS-Sp4ce/AWVS11.X-Chinese-Version awvs11 汉化包
```

Burpsuit 相关工具拓展插件

```
https://github.com/PortSwigger burpsuite 官方插件库
https://github.com/snoopysecurity/awesome-burp-extensions awesome 系列之 burp 拓展
https://github.com/d3vilbug/HackBar 集成 hackbar
https://github.com/PortSwigger/turbo-intruder 比 Burp 自带的 Intruder 更快，一分钟打 1.61 万次请求
https://github.com/Ebryx/AES-Killer burp 插件，破解 aes 加密的插件
https://github.com/bugcrowd/HUNT 可以将 burpsuite 扫描器功能扩展的更加强大，同时支持 zapproxy 扩展
https://github.com/wagiro/BurpBounty burp 插件增强主动与被动扫描功能
https://github.com/nccgroup/BurpSuiteHTTPSmuggler Burp 拓展，使用几种技巧绕过 WAF
https://github.com/PortSwigger/command-injection-attacker burp 插件，命令注入漏洞检测
https://github.com/nccgroup/freddy burp 插件，自动识别 Java/.NET 应用程序中的反序列化漏洞
https://github.com/modzero/interestingFileScanner burp 插件，增强敏感文件扫描
https://github.com/summitt/Burp-Non-HTTP-Extension burp 插件，布置 dns 服务器抓取流量
https://github.com/ilmila/J2EEScan burp 拓展，扫描 J2EE 应用
https://github.com/JGillam/burp-co2 集成了 sqlmap，菜刀，字典生成等
https://github.com/swisskyrepo/SSRFmap burp 插件，检测 ssrf 漏洞
```

Sqlmap 相关工具拓展插件

```
https://github.com/codewatchorg/sqlipy burp 与 sqlmap 联动插件
https://github.com/Hood3dRob1n/SQLMAP-Web-GUI sqlmap 的 web gui
https://github.com/KINGSABRI/sqlmap-tamper-api 利用各种语言来编写 sqlmapTamper
https://github.com/0xbug/SQLiScanner 一款基于 sqlmapapi 和 Charles 的被动 SQL 注入漏洞扫描工具
https://github.com/fengxuangit/Fox-scan 基于 sqlmapapi 的主动和被动资源发现的漏洞扫描工具
https://github.com/UltimateHackers/sqlmate 在 sqlmap 基础上增加了目录扫描、hash 爆破等功能
https://github.com/ysrc/GourdScanV2 ysrc 出品的被动式漏洞扫描工具，基于 sqlmapapi
https://github.com/zt2/sqli-hunter 基于 sqlmapapi，ruby 编写的漏洞代理型检测工具
https://github.com/jesuiscamille/AutoSQLi 利用 DorkNet，Googler，Ddgr，WhatWaf 和 sqlmap 自动注入
```

Nmap 相关工具拓展插件

```
https://github.com/Ullaakut/nmap GO，实现的 Nmap 调用库
https://github.com/cldrn/nmap-nse-scripts NSE 收集列表
https://github.com/vulnersCom/nmap-vulners 使用 nmap 扫描常见的服务漏洞
https://github.com/s4n7h0/Halcyon Nmap Script (NSE)IDE 编辑器
https://github.com/m4ll0k/AutoNSE NSE 自动化利用
https://github.com/Screetsec/Dracnmap shell，将 Nmap 复杂的命令进行一定程度的集成与简化，使新用户更加容易上手。
https://github.com/cldrn/rainmap-lite Django，Web 版 Nmap，可以建立新的扫描服务器，允许用户从他们的手机/平板电脑/网络浏览器启动 Nmap 扫描
https://github.com/trimstray/sandmap linux 下将支持使用大量 Nmap 引擎进行网络和系统侦察的工具
https://github.com/m0nad/HellRaiser 基于 nmap 的扫描器，与 cve 漏洞关联
https://github.com/scipag/vulscan 基于 nmap 的高级漏洞扫描器，命令行环境使用
https://github.com/Rev3rseSecurity/WebMap 将 nmap 的 xml web 展示器
https://github.com/DanMcInerney/msf-autopwn 执行 NMap 扫描或读取扫描结果，然后自动使用 msf 攻击包含常见漏洞的主机
```

Metasploit 相关工具拓展插件

```
https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit 结合机器学习与 msf 的全自动测试工具
https://github.com/r00t-3xp10it/Meterpreter_Paranoid_Mode-SSL 一个可以创建 SSL/TLS shell 连接的脚本
https://github.com/DanMcInerney/msf-netpwn 等待 msf 的 session，并自动提为域管理
https://www.exploit-db.com/exploits/45851/ msf 插件，利用 jira upm 上传进行命令执行
https://github.com/NullArray/AutoSploit 利用 Shodan 搜索引擎收集目标，并自动调用设定的 msf 模块对目标发动攻击
https://github.com/WazeHell/metateta 使用 msf 脚本，根据特定协议进行扫描
https://github.com/fbkcs/msf-elf-in-memory-execution Metasploit 模块，用于在内存中执行 ELF 文件
https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit metasploit 双星攻击利用文件
https://github.com/darkoperator/Metasploit-Plugins msf 扩展资产搜集与帮助插件
https://github.com/D4Vinci/One-Lin3r metasploit、payload 辅助查询工具
https://github.com/shizzz477/msploitego 将 msf 数据库与 maltego 进行图形化展示
https://github.com/scriptjunkie/msfgui metasploit 的 GUI 界面，话说现在 msf 对 windows 支持也挺好的
```

CobaltStrike 相关工具拓展插件

```
https://mp.weixin.qq.com/s/CEI1XYkq2PZmYsP0DRU7jg 使用 Aggressor 脚本雕饰 Cobalt Strike
https://github.com/rsmudge/armitage CobaltStrike 社区版，调用 msf，一对多带界面
https://github.com/anbai-inc/CobaltStrike_Hanization CobaltStrike2.5 汉化版，以 msf 库为基础，3.0 以后改版
https://github.com/rsmudge/cortana-scripts 用于 cs2.x 与 armitage 的可拓展插件，cvs3.x 的为 AggressorScripts
https://github.com/harleyQu1nn/AggressorScripts cs3.0 以后的脚本搜集
https://github.com/FortyNorthSecurity/AggressorAssessor cs3.x 自动化攻击脚本集合
https://github.com/Ridter/CS_Chinese_support/ cs3.0 传输信息的汉化插件
https://github.com/verctor/CS_xor64 生成 cobaltstrike 所需的 xor64.bin
https://github.com/ryhanson/ExternalC2 一个用于将通信渠道与 Cobalt Strike External C2 服务器集成的库
https://github.com/threatexpress/cs2modrewrite 用于将 Cobalt Strike 配置文件转换为 mod_rewrite 脚本的工具
https://github.com/Mr-Un1k0d3r/CatMyFish 搜索分类域，为 Cobalt Strike beacon C&C 设置白名单域
https://github.com/threatexpress/malleable-c2 利用 jquery 文件进行 C2 通讯，在文件内做了 JS 混淆绕过防火墙
https://github.com/dcsync/pycobalt py3,Python API for Cobalt Strike
https://www.cobaltstrike.com/aggressor-script/cobaltstrike.html CobaltStrike 相关插件编写，一对多带界面
```

Empire 相关工具拓展插件

```
https://paper.tuisec.win/detail/f3dce68a0b4baaa 利用 Empire 获取域控权限
https://github.com/EmpireProject/Empire-GUI empire 的 node.js 界面
https://github.com/interference-security/empire-web empire 的 web 界面
https://github.com/byt3bl33d3r/DeathStar py3,调用 Empire RESTful API 自动化获取域管权限的
https://github.com/infosecn1nja/e2modrewrite 用于将 Empire 配置文件转换为 Apache modrewrite 脚本
https://github.com/maxchehab/CSS-Keylogging Chrome 扩展程序和 Express 服务器利用 CSS 的键盘记录功能。
https://github.com/evilcos/cookiehacker Chrome 扩展程序。JavaScript document.cookie / Wireshark Cookie
https://github.com/lfzark/cookie-injecting-tools Chrome 扩展，cookie 注入工具包括注入，编辑，添加和删除 cookie
```

信息搜集

https://github.com/smicallef/spiderfoot 利用 OSINT 自动化找出对方信息，gui 界面，插件化
https://github.com/Nhoya/gOSINT go，利用 OSINT 自动化搜集信息
https://github.com/laramies/theHarvester 企业被搜索引擎收录敏感资产信息监控脚本：员工邮箱、子域名、Hosts
https://github.com/guelfoweb/knock 通过爆破进行子域名获取，可用于查找子域名接管漏洞
https://github.com/aboul3la/Sublist3r 通过搜索引擎与爆破快速子域枚举工具
https://github.com/Ice3man543/subfinder 基于 go 实现的 Sublist3r
https://github.com/yanxiu0614/subdomain3 py3、py2 的子域名,IP,CDN 信息等
https://github.com/caffix/amass 基于 go，子域名枚举，搜索互联网数据源，使用机器学习猜测子域名
https://github.com/nahamsec/lazyrecon 侦查 reconnaissance 过程自动化脚本，可自动使用 Sublist3r/certspotter 获取子域名，调用 nmap/dirsearch 等
https://github.com/s0md3v/ReconDog simple，侦查信息的瑞士军刀
https://github.com/FeeiCN/ESD py3，爆破搜集子域名
https://github.com/alpha1e0/pentestdb 多用途集成化信息搜集工具
https://github.com/se55i0n/PortScanner py2,目标 tcp 端口快速扫描、banner 识别、cdn 检测
https://github.com/lijiejie/subDomainsBrute lijiejie 开发的一款使用广泛的子域名爆破枚举工具
https://github.com/ring04h/wydomain 猪猪侠开发的一款域名收集全面、精准的子域名枚举工具
https://github.com/n4xh4ck5/N4xD0rk 利用搜索引擎来搜集子域名，可以使用西班牙语搜集
https://github.com/vysec/DomLink py2,调用 WHOXY.com，对邮箱和域名进行进一步的搜集
https://github.com/jonluca/Anubis py3.6，子域名爆破与信息搜集
https://github.com/le4f/dnsmaper web 界面，子域名枚举爆破工具以及地图位置标记
https://github.com/thewhiteh4t/seeker 获取高精度地理信息和设备信息的工具
https://github.com/0xbug/orangescan web 界面，的在线子域名信息收集工具
https://github.com/TheRook/subbrute 扫描器中常用的子域名爆破 API 库
https://github.com/We5ter/GSDF 基于谷歌 SSL 透明证书的子域名查询脚本
https://github.com/mandatoryprogrammer/cloudflare_enum 利用 CloudFlare 的 dns 进行子域名枚举
https://github.com/ultrasecurity/webkiller 渗透辅助，py，ip 信息、端口服务指纹、蜜罐探测、bypass cloudflare
https://github.com/christophetd/CloudFlair cloudflare 绕过，获取真实 ip，集成 censys
https://github.com/exp-db/PythonPool/tree/master/Tools/DomainSeeker 多方式收集目标子域名信息
https://github.com/code-scan/BroDomain 子域名查询
https://github.com/michenriksen/aquatone 子域名枚举、探测工具。可用于子域名接管漏洞探测
https://github.com/chuhades/dnsbrute 基于 go，高效的子域名爆破工具
https://github.com/evilsocket/dnssearch 基于 go，一款子域名爆破工具
https://github.com/OJ/gobuster 基于 go，根据 dns 查询子域名和 web 目录爆破的工具
https://github.com/reconned/domained 可用于子域名收集的一款工具
https://github.com/bit4woo/Teemo 多方式域名收集及枚举工具
https://github.com/swisskyrepo/Subdomino 子域名枚举，端口扫描，服务存活确认
https://github.com/nmalcolm/Inventus 通过爬虫实现的子域名收集工具
https://github.com/alienwithin/OWASP-mth3l3m3nt-framework 渗透辅助，php，exp 搜寻、payload 与 shell 生产、信息搜集
https://github.com/chrismaddalena/ODIN py3，simple，信息搜集与后期漏洞利用
https://github.com/x0day/bannerscan C 段/旁站查询与路径扫描
https://github.com/Xyntax/BingC 基于 Bing 搜索引擎的 C 段/旁站查询，多线程，支持 API
https://github.com/zer0h/httpscan 网段 Web 主机发现小工具
https://github.com/lijiejie/BBScan 网站信息泄漏批量扫描脚本
https://github.com/aipengjie/sensitivefilescan 网站敏感文件扫描工具
https://github.com/Mosuan/FileScan 网站敏感文件扫描 / 二次判断降低误报率 / 扫描内容规则化 / 多目录扫描
https://github.com/Xyntax/FileSensor 网站敏感文件探测工具
https://github.com/ring04h/weakfilescan 多线程网站泄露信息检测工具
https://github.com/Viralmaniar/Passhunt simple，用于搜索网络设备 Web 应用程序等的默认凭证。包含 523 个厂家的 2084 组默认密码
https://github.com/yassineaboukir/Asnlookup simple,利用 ASN 搜索特定组织拥有 ip，可联动 nmap、masscan 进行进一步信息扫描

敏感信息泄露发现

https://github.com/Yelp/detect-secrets PY,防止代码中的密码等相关敏感信息被提交到代码库中，可以在保证安全性的同时不会给开发者的生产力带来任何影响
https://github.com/Acceis/leakScraper 处理和可视化大规模文本文件，查找敏感信息，例如证书
https://github.com/Raikia/CredNinja 多线程用户凭证验证脚本，比如验证 dump 的 hash 是否属于此机器，利用 445 端口进行协议验证
https://github.com/CERTCC/keyfinder 查找并分析私钥/公钥文件(文件系统中)，支持 Android APK 文件
https://github.com/Ice3man543/hawkeye go，cli 端，文件系统分析工具，快速查找文件内包含的 SSH 密钥，日志文件，Sqlite 数据库，密码文件等
https://github.com/FortyNorthSecurity/EyeWitness 获取目标网站截图、vnc、rdp 服务，尝试获取默认凭证
https://github.com/D4Vinci/Cr3dOv3r 根据邮箱自动搜索泄漏的密码信息，也可测试账户密码在各大网站能否登录的工具

威胁情报分析

https://www.databases.today，https://publicdbhost.dmca.gripe/，http://www.wttech.org/，https://hashes.org/leaks.php，https://archive.org/search.php?query= 密码泄露
https://www.threatcrowd.org/ 威胁情报分析平台
https://x.threatbook.cn/ 微步在线 | 威胁情报分析平台-ThreatBook-多引擎在线扫描、恶意软件在线检测
https://github.com/needmorecowbell/sniff-paste 针对 Pastebin 的开源情报收集工具
https://talosintelligence.com/documents/ip-blacklist 恶意 IP 地址
https://ransomwaretracker.abuse.ch/downloads/RW_IPBL.txt 恶意软件 IP 地址
https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1 洋葱路由出口节点
https://isc.sans.edu/api/threatlist/shodan shodan 撒旦扫描器节点
https://github.com/Te-k/harpoon 用于开源和威胁智能的 CLI 工具
https://trumail.io/ 验证对方邮箱是否为垃圾邮箱，每个月可以免费验证 1000 次
https://github.com/ChrisJohnRiley/Scythe 验证账号是否为常用账号
https://github.com/fireeye/GeoLogonalyzer 远程身份验证地理位置分析工具，用于区分合法登录和恶意登录。
https://github.com/target/strelka py3，通过实时扫描文件进行威胁情报分析和实时监测。

托管云安全

https://github.com/stuhirst/awssecurity/blob/master/arsenal.md AWS 安全检测相关的项目列表
https://github.com/toniblyx/my-arsenal-of-aws-security-tools AWS 安全工具集
https://github.com/sa7mon/S3Scanner 扫描 amazon 公开的 S3 buckets 和 dump
https://github.com/kromtech/s3-inspector 检测亚马逊 AWS S3 bucket permissions
https://github.com/jordanpotti/AWSBucketDump 枚举 AWS S3 buckets 以查找敏感机密的文件
https://github.com/sa7mon/S3Scanner 扫描 amazon 公开的 S3 buckets 和 dump
https://github.com/kromtech/s3-inspector 检测亚马逊 AWS S3 bucket permissions
https://github.com/jordanpotti/AWSBucketDump 枚举 AWS S3 buckets 以查找敏感机密的文件
https://github.com/Netflix/repokid AWS 最低权限策略部署工具
https://github.com/RhinoSecurityLabs/pacu AWS 漏洞检测框架
https://github.com/0xbug/Hawkeye GitHub 泄露监控系统
https://github.com/neal1991/gshark github 信息泄露检测
https://github.com/VKSRC/Github-Monitor GitHub 监控，代码信息泄露，分钟级监控，邮件预警
https://github.com/metac0rtex/GitHarvester github Repo 信息搜集工具
https://github.com/repoog/GitPrey GitHub 敏感信息扫描工具
https://github.com/FeeiCN/GSIL py3，近实时监控 Github 敏感信息，并发送告警通知。
https://github.com/UnkL4b/GitMiner github 敏感内容挖掘
https://github.com/dxa4481/truffleHog GitHub 敏感信息扫描工具,包括检测 commit 等
https://github.com/Hell0W0rld0/Github-Hunter github 信息监测脚本
https://github.com/awslabs/git-secrets 防止将敏感数据提交到 git 仓库的工具
https://github.com/zricethezav/gitleaks 基于 go 的，检查 git repo 中的密码信息和密钥

目录路径发现

https://github.com/maurosoria/dirsearch 经典目录路径扫描
https://github.com/TheM4hd1/PenCrawLer C#界面，web 爬虫与目录路径爆破工具，除了常规扫描增加了递归爆破模式
https://github.com/Xyntax/DirBrute 目录路径爆破工具
https://github.com/abaykan/crawlbox 目录路径路径扫描器
https://github.com/deibit/cansina 目录路径路径扫描器
https://github.com/UltimateHackers/Breacher 多线程的后台路径扫描器，也可用于发现 Execution After Redirect 漏洞
https://github.com/fnk0c/cangibrina 通过字典穷举、google、robots.txt 等途径的跨平台后台管理路径扫描器
https://github.com/Go0s/SitePathScan 基于协程的目录路径爆破工具，配合 aiohttp 扫描路径比之前快了三倍有余
https://github.com/secfree/bcrpscan 基于爬虫的 web 路径扫描器

本地文件包含漏洞

https://github.com/hvqzao/liffy 本地文件包含漏洞利用工具
https://github.com/D35m0nd142/Kadabra 本地文件包含漏洞扫描和利用工具
https://github.com/P0cL4bs/Kadimus 本地文件包含漏洞扫描和利用工具
https://github.com/D35m0nd142/LFISuite 本地文件包含漏洞利用及扫描工具，支持反弹 shell
https://github.com/OsandaMalith/LFiFreak 本地文件包含漏洞利用及扫描工具，支持反弹 shell

安全测试与扫描器框架

https://github.com/zaproxy/zaproxy The OWASP ZAP core project 出品的综合性渗透测试工具。由于其流量代理、请求重放和可扩展性拿来做模糊测试未尝不可
https://github.com/x-Ai/BurpUnlimitedre burpsuite 1.7.27 的永久破解版
https://github.com/andresriancho/w3af 知名插件化扫描器
https://github.com/juansacco/exploitpack 渗透测试集成框架，包含超过 38,000+ exploits
https://github.com/Lucifer1993/AngelSword Web 应用漏洞扫描框架,python3，300poc
https://github.com/Xyntax/POC-T 渗透测试插件化扫描框架，自带 poc，并发扫描
https://github.com/knownsec/Pocsuite 知道创宇维护的一个规范化 POC/EXP 利用框架
https://github.com/leisurelicht/Pocsuite3 Pocsuite 用 py3 重写
https://github.com/Eitenne/roxysploit 漏洞利用框架，支持永恒之蓝直接利用
https://github.com/TophantTechnology/osprey 斗象能力中心出品并长期维护的一个规范化 POC/EXP 利用框架
https://github.com/he1m4n6a/btScan 大黑阔的插件化漏洞利用工具
https://github.com/boy-hack/w9scan python 下内置 1200+插件可对网站进行一次规模的检测
https://github.com/WooYun/TangScan 乌云维护的一个规范化 POC/EXP 利用框架
https://github.com/n0tr00t/Beebeeto-framework Beebeeto 是由众多安全研究人员所共同维护的一个规范化 POC/EXP 利用框架
https://github.com/erevus-cn/pocscan 一款开源 Poc 调用框架,可轻松调用 Pocsuite,Tangscan,Beebeeto,Knowsec 老版本 POC，可使用 docker 部署
https://github.com/DavexPro/PocHunter 借鉴 pocscan 的一款多利用框架 poc 适配框架
https://github.com/theInfectedDrake/TIDoS-Framework 覆盖从侦察到漏洞分析的所有内容
https://github.com/gyoisamurai/GyoiThon 使用深度学习的渗透测试工具，从每次扫描数据中学习，扫描越多，软件检测精准度越高
https://github.com/euphrat1ca/polar-scan 易语言的北极熊扫描器
https://github.com/euphrat1ca/yeezy-scan 椰树 1.9 扫描器
https://github.com/euphrat1ca/WebCruiserWVS 轻量级基于 C#的扫描器，椰树扫描器的前身
https://github.com/Skycrab/leakScan web 界面，漏洞扫描
https://github.com/az0ne/AZScanner web 界面，自动漏洞扫描器，子域名爆破，端口扫描，目录爆破，常用框架漏洞检测
https://github.com/boy-hack/w8scan web 界面，基于 bugscan 扫描和架构思想的扫描器
https://github.com/MiniSafe/microweb web 界面，base bugscan，django
https://github.com/taipan-scanner/Taipan web 界面，基于 F#与 C#的安全扫描器
https://github.com/zhangzhenfeng/AnyScan web 界面，python 漏洞扫描器
https://github.com/Canbing007/wukong-agent web 界面，python 漏洞扫描器
https://github.com/dermotblair/webvulscan web 界面，php，漏洞扫描器，支持输出 pdf 报告
https://github.com/jeffzh3ng/InsectsAwake web 界面，基于 Flask 应用框架的漏洞扫描系统，同时集成了渗透测试常用的端口扫描、子域名爆破等功能，后端漏洞扫描采用 Pocsuite
https://github.com/0xInfection/TIDoS-Framework py，linux，网站扫描器
https://github.com/secdec/adapt py,linux，网站扫描器
https://github.com/sullo/nikto perl，linux，kali 内置的网站扫描器
https://github.com/Ekultek/Zeus-Scanner web 扫描器，联动 Geckodriver，nmap 和 sqlmap
https://github.com/blackye/lalascan 集合 owasp top10 漏洞扫描和边界资产发现能力的分布式 web 漏洞扫描框架
https://github.com/blackye/BkScanner BkScanner 分布式、插件化 web 漏洞扫描器

```
https://github.com/tlkh/prowler 一款基于 Raspberry Pi Cluster 的网络漏洞扫描工具
https://github.com/netxfly/passive_scan 基于 http 代理的 web 漏洞扫描器
https://github.com/1N3/Sn1per php，自动化中间件扫描以及设备指纹识别
https://github.com/Tuhinshubhra/RED_HAWK php，集成信息收集、漏洞扫描、指纹识别等的扫描工具
https://github.com/m4ll0k/Spaghetti web 应用扫描器，支持指纹识别、文件目录爆破、SQL/XSS/RFI 等漏洞扫描，也可直接用于 str
uts、ShellShock 等漏洞扫描
https://github.com/v3n0m-Scanner/V3n0M-Scanner 支持检测 SQLi/XSS/LFI/RFI 等漏洞的扫描器
https://github.com/Yukinoshita47/Yuki-Chan-The-Auto-Pentest 集成子域名枚举、nmap、waf 指纹识别等模块的 web 应用扫描器
https://github.com/RASSec/pentestEr_Fully-automatic-scanner 定向自动测试工具
https://github.com/Fireflyi/lcyscan py，插件化漏洞扫描器，支持生成报表
https://github.com/Arachni/arachni Web 应用漏洞扫描框架，支持 REST、RPC 等 api 调用
https://github.com/swisskyrepo/DamnWebScanner 基于 chrome/opera 插件的被动式漏洞扫描
https://github.com/0xsauby/yasuo ruby,扫描主机第三方 web 应用服务漏洞
https://github.com/yangbh/Hammer Web 应用漏洞扫描
https://github.com/viraintel/OWASP-Nettacker 自动化渗透测试框架
https://github.com/flipkart-incubator/watchdog 全面的 web 扫描器与漏洞利用工具
https://github.com/Fplyth0ner-Combie/Bug-Project-Framework 易语言，模仿 msf 的漏洞利用框架，自带 exp 编辑器
https://github.com/PowerScript/KatanaFramework py，模仿 msf 的漏洞利用框架，还有些 ssh、压缩包破解工具
https://github.com/m4ll0k/Galileo py2，网站扫描器
https://github.com/samhaxr/hackbox py2，simple，网站扫描器
https://github.com/secrary/EllaScanner py3，simple，被动式漏洞扫描，支持历史 cve 编号漏洞识别
https://github.com/m4ll0k/WAScan py，simple，扫描页面/链接/脚本/Form，测试 Payload 等
https://github.com/jiangsir404/S7scan py,已用 1，七种综合检测
https://github.com/hatRiot/clusterd py，simple，web 漏洞利用
https://github.com/M4cs/BabySploit py,simple,模仿 msf
https://github.com/iceyhexman/onlinetools simple，web 界面，在线 cms 指纹识别|旁站|c 段|信息泄露|工控|系统|物联网安全|
cms 漏洞扫描|端口扫描|等
https://github.com/tulpar/tulpar simple,支持多种 web 漏洞扫描
https://github.com/UltimateHackers/Striker simple，信息搜集、cms 利用与漏扫，侦察绕过 Cloudflare
https://github.com/0x4D31/salt-scanner 基于 Salt Open 以及 Vulners Linux Audit API 的 linux 漏洞扫描器，支持与 JIRA
、slack 平台结合使用
https://github.com/opensec-cn/kunpeng go，POC 检测框架，以动态链接库的形式提供各种语言调用
```

运维安全服务与资产管理

https://github.com/chaitin/cloudwalker CloudWalker（牧云）服务器安全管理平台，逐步覆盖服务器资产管理、威胁扫描、Webshell 查杀、基线检测等功能。
https://github.com/mitre/caldera mitre 公司模拟攻击测试系统，主要是在 win 下
https://github.com/guardicore/monkey 评估网络安全状况，分为扫描器与 C2C 服务器，利用默认口令与 exp 对 ssh、smb 等多种协议方式进行攻击检测
https://github.com/grayddq/PublicSecScan 调用 awvs 对大量 WEB 资产进行分布式 WEB 安全扫描，发现 web 环境下常规的一些安全漏洞
https://github.com/jeffzh3ng/Fuxi-Scanner 资产管理，漏洞检测集成 awvs、创宇 Pocsuite、nmap、hydra
https://github.com/infobyte/faraday 协作渗透测试和漏洞管理平台，集成多种
https://github.com/DefectDojo/django-DefectDojo 基于 django 的漏洞资产管理平台
https://github.com/creditease-sec/insight web 界面，宜信安全部开发，集成应用系统资产管理、漏洞全生命周期管理、安全知识库管理三位一体的管理平台
https://github.com/RASSec/A_Scan_Framework 漏洞管理、资产管理、任务扫描系统
https://github.com/cea-sec/ivre 网络资产指纹发现，搭建属于自己的 shodan 与 zoomeye
https://github.com/ysrc/xunfeng web 界面，同程安全开发的网络资产识别引擎，漏洞检测引擎
https://github.com/superhuahua/xunfengES web 界面，base 巡风开发，一个人的安全
https://github.com/zhaoweiho/SecurityManageFramwork py3，django。企业内网安全管理平台，包含资产管理，漏洞管理，账号管理，知识库管、安全扫描自动化功能模块
https://github.com/grayddq/PublicMonitors 对公网 IP 列表进行端口服务扫描，发现周期内的端口服务变化情况和弱口令安全风险。一个人的安全部
https://github.com/grayddq/PubilcAssetInfo 主要目标是以甲方安全人员的视角，尽可能收集发现企业的域名和服务器公网 IP 资产。如百度云、阿里云、腾讯云等。一个人的安全部
https://github.com/maya6/SiteScan web 界面，py3 celery。资产收集
https://github.com/ywolf/F-NAScan py2.6，网络资产、端口服务搜集整理，生成报表显示。快速
https://github.com/flipkart-incubator/RTA 扫描公司内部所有在线设备，提供整体安全视图，标示所有安全异常
https://github.com/0xbug/Biu-framework 企业内网基础服务安全扫描框架

上传漏洞利用

https://github.com/UltimateHackers/Arjun 扫描网页，使用正则表达式爆破查找隐藏的 GET/POST 参数
https://github.com/3xp10it/xupload 用于自动测试上传功能是否可上传 webshell 的工具
https://github.com/gunnerstahl/JQShell py3，CVE-2018-9206 jQuery File Upload 利用工具
https://github.com/destine21/ZIPFileRaider burp 插件，测试 zip 文件上传漏洞
https://github.com/jpiechowka/zip-shotgun py，测试 zip 文件上传漏洞

端口发现服务指纹识别

```
https://github.com/nmap/nmap LUA,Nmap 端口扫描器，具有有强大的脚本引擎框架
https://github.com/robertdavidgraham/masscan C,无状态扫描，可以调用 nmap 进行指纹识别
https://github.com/zmap/zmap C,无状态扫描，需要用 C 编写扩展模块
https://github.com/zmap/zgrab go，基于 zmap 扫描器进行指纹识别、调度管理，可绕过 CDN
https://github.com/chichou/grab.js 类似 zgrab 的快速 TCP 指纹抓取解析工具，支持更多协议
https://github.com/johnnyxmas/scancannon shell,联动 masscan 和 nmap
https://github.com/OffensivePython/Nscan 基于 Masscan 和 Zmap 的网络扫描器
https://github.com/ring04h/wyportmap 调用 nmap 目标端口扫描+系统服务指纹识别
https://github.com/angryip/ipscan Angry IP Scanner，跨平台界面化端口扫描器
https://github.com/EnableSecurity/wafw00f WAF 产品指纹识别
https://github.com/rbsec/sslscan ssl 类型识别
https://github.com/urbanadventurer/whatweb web 指纹识别
https://github.com/Rvn0xsy/FastWhatWebSearch whatweb 工具结果搜索平台
https://github.com/tanjiti/FingerPrint web 应用指纹识别
https://github.com/nanshihui/Scan-T 网络爬虫式指纹识别
https://github.com/ywolf/F-MiddlewareScan 中间件扫描服务识别
https://github.com/lietdai/doom thorn 上实现的分布式任务分发的 ip 端口漏洞扫描器
https://github.com/RASSec/RASscan 端口服务扫描
https://github.com/m3liot/shcheck 用于检查 web 服务的 http header 的安全性
https://github.com/mozilla/ssh_scan 服务器 ssh 配置信息扫描
https://github.com/18F/domain-scan 针对域名及其子域名的资产数据检测 / 扫描，包括 http/https 检测等
https://github.com/ggusoft/inforfinder 域名资产收集及指纹识别工具
https://github.com/0xbug/Howl 网络设备 web 服务指纹扫描与检索
https://github.com/mozilla/cipherscan 目标主机服务 ssl 类型识别
https://github.com/medbenali/CyberScan 渗透测试辅助工具，支持分析数据包、解码、端口扫描、IP 地址分析等
https://github.com/jekyc/wig web 应用信息搜集工具
https://github.com/eldraco/domain_analyzer 围绕 web 服务的域名进行信息收集和”域传送”等漏洞扫描，也支持针对背后的服务器端口扫描等
https://github.com/cloudtracer/paskto 基于 Nikto 扫描规则的被动式路径扫描以及信息爬虫
https://github.com/zerokeeper/WebEye 快速识别 WEB 服务器类型、CMS 类型、WAF 类型、WHOIS 信息、以及语言框架
https://github.com/n4xh4ck5/CMSsc4n CMS 指纹识别
https://github.com/HA71/WhatCMS CMS 检测和漏洞利用脚本，基于 Whatcms.org API
https://github.com/boy-hack/gwhatweb CMS 识别 python gevent 实现
https://github.com/wpscanteam/wpscan 基本算是 word press 下最好用的工具了
https://github.com/swisskyrepo/Wordpresscan 基于 WPScan 以及 WPSeku 的优化版 wordpress 扫描器
https://github.com/m4ll0k/WPSeku 精简的 wordpress 扫描工具
https://github.com/rastating/wordpress-exploit-framework wordpress 漏洞利用框架
https://github.com/Jamalc0m/wphunter php，wordpress 扫描器
https://github.com/UltimateLabs/Zoom wordpress 漏洞扫描器
https://github.com/immunIT/drupwn Drupal 信息收集与漏洞利用工具
https://github.com/CHYbeta/cmsPoc CMS 渗透测试框架
https://github.com/chuhades/CMS-Exploit-Framework CMS 攻击框架
https://github.com/Tuhinshubhra/CMSeeK 20 多种 CMS 的基本检测，针对 wp 利用、可定制模块化爆破功能
https://github.com/Dionach/CMSmap 支持 WordPress，Joomla 和 Drupal 扫描
https://github.com/Moham3dRiahi/XAttacker Web CMS Exploit 工具,包含针对主流 CMS 的 66 个不同的 Exploits
https://github.com/code-scan/dzscan 首款集成化的 Discuz 扫描工具
```

数据库扫描与爆破

```
https://github.com/ron190/jsql-injection Java 编写的 SQL 注入工具
https://github.com/shack2/SuperSQLInjectionV1 安恒航牛的一款界面化注入工具
https://github.com/sqlmapproject/sqlmap sql 注入 sqlmap
https://github.com/stamparm/DSSS 已用 1,99 行代码实现的 sql 注入漏洞扫描器
https://github.com/Hadesy2k/sqliv 已用 1,基于搜索引擎的批量 SQL 注入漏洞扫描器
https://github.com/quentinhardy/odat 一款专门用于 Oracle 渗透的很全面的工具
https://github.com/m8r0wn/enumdb MySQL 和 MSSQL 利用工具后期爆破、搜索数据库并提取敏感信息。
https://github.com/LoRexxar/Feigong 针对各种情况自由变化的 MySQL 注入脚本
https://github.com/youngyangyang04/NoSQLAttack 一款针对 mongoDB 的攻击工具
https://github.com/Neohapsis/bbqsql SQL 盲注利用框架
https://github.com/NetSPI/PowerUpSQL 基于 Powershell 的 sqlserver 测试框架
http://www.4hou.com/system/14950.html 利用 PowerUpSQL，渗透测试技巧：绕过 SQL Server 登录触发器限制
https://github.com/WhitewidowScanner/whitewidow 一款数据库扫描器
https://github.com/stampery/mongoaudit MongoDB 审计及渗透工具
https://github.com/torque59/Nosql-Exploitation-Framework NoSQL 扫描/爆破工具
https://github.com/missDronio/blindy MySQL 盲注爆破工具
https://github.com/JohnTroony/Blisqy 用于 http header 中的时间盲注爆破工具，仅针对 MySQL/MariaDB
https://github.com/se55i0n/DBScanner 自动扫描内网中常见 sql、no-sql 数据库脚本，包含未授权访问及常规弱口令检测
https://github.com/Turr0n/firebase 对没有正确配置的 firebase 数据库进行利用
```

XSS 跨站脚本检测利用

```
https://github.com/UltimateHackers/AwesomeXSS XSS Awesome 系列
http://www.xss-payloads.com 很全面的 xss 工具包与资料
https://github.com/ismailtasdelen/xss-payload-list XSS 漏洞 Payload 列表
https://github.com/beefproject/beef 经典的 xss 利用框架
https://github.com/samdenty99/injectify 类似 beef 的 xss 利用框架
https://github.com/firesunCN/BlueLotus_XSSReceiver 蓝莲花战队为 CTF 打造的 xss 利用框架
https://github.com/NytroRST/XSSFuzzer 根据特定标签生成 xss payload
https://github.com/evilcos/xssor2 余弦写的 xss 利用辅助工具
https://github.com/UltimateHackers/XSStrike 可识别并绕过 WAF 的 XSS 扫描工具
https://github.com/raz-varren/xsshell go,利用 xss 漏洞返回一个 js 交互 shell
https://github.com/UltimateHackers/JShell 利用 xss 漏洞返回一个 js 交互 shell
https://github.com/shawarkhanethicalhacker/BruteXSS 一款 XSS 扫描器,可暴力注入参数
https://github.com/1N3/XSSTracer 小型 XSS 扫描器,也可检测 CRLF、XSS、点击劫持的
https://github.com/0x584A/fuzzXssPHP PHP 版本的反射型 xss 扫描
https://github.com/chuhades/xss_scan 批量扫描 XSS 的 python 脚本
https://github.com/BlackHole1/autoFindXssAndCsrf 自动化检测页面是否存在 XSS 和 CSRF 漏洞的浏览器插件
https://github.com/shogunlab/shuriken 使用命令行进行 XSS 批量检测
https://github.com/stamparm/DSXS 支持 GET、POST 方式的高效 XSS 扫描器
https://github.com/bsmali4/xssfork kali 下无法使用的话，请下载正确的 PhantomJS 到目录 thirdparty/phantomjs/Linux
https://github.com/riusksk/FlashScanner flash xss 扫描
https://github.com/Damian89/xssfinder 针对检测网站中的反射 XSS
https://github.com/BlackHole1/WebRtcXSS 自动化利用 XSS 入侵内网
```

弱口令扫描爆破

```
https://github.com/vanhauser-thc/thc-hydra 支持多种协议方式的破解与爆破，v8 以后就不提供 windows 版本了
https://github.com/nmap/ncrack c，支持多种协议的破解与爆破
https://github.com/0pn1i9ht/F-Scrack ysrc 对各类服务用户名密码爆破的脚本
https://github.com/TunisianEagles/SocialBox 针对 fb、gmail、ins、twitter 的用户名密码爆破的脚本
https://github.com/lanjelot/patator 支持多种协议的爆破，采用模块化设计，使用灵活
https://github.com/m4ll0k/SMBrute 利用 smb 服务进行用户名密码爆破
https://github.com/netxfly/crack_ssh Go 写的协程版的 ssh\redis\mongodb 弱口令破解
https://github.com/UltimateHackers/Blazy 支持测试 CSRF，Clickjacking，Cloudflare and WAF 的弱口令探测器
https://github.com/Moham3dRiahi/XBruteForcer WordPress、Joomla、DruPal、OpenCart、Magento 等 CMS 用户密码爆破
https://github.com/shengqi158/weak_password_detect Linux 下利用 nmap 多线程探测 ssh 弱口令
https://github.com/ztgrace/changeme 弱口令扫描器，不仅支持普通登录页，也支持 ssh、mongodb 等组件
https://github.com/lijiejie/htpwdScan simple，http 暴力破解、撞库攻击脚本
https://github.com/scu-igroup/ssh-scanner 联动 nmap、hydra 对 ssh 批量爆破
```

密码破解还原

```
https://securityxploded.com/download.php 各种密码方向安全小工具
https://github.com/bdutro/ibm_pw_clear IBM x3550/x3560 M3 bios 密码清除重置工具
https://github.com/thehappydinoa/iOSRestrictionBruteForce py,实现的 ios 访问限制密码破解工具
https://github.com/hashcat/hashcat C,哈希破解
https://github.com/fireeye/gocrack GO,基于 hashcat 3.6.0+的分布式密码破解工具
https://github.com/s3inlc/hashtopolis 基于 php 的 hashcat 的分布式破解工具，支持 C#与 python 客户端
https://github.com/e-ago/bitcracker 首款开源的 BitLocker 密码破解工具
https://www.ru.nl/publish/pages/909282/draft-paper.pdf 破解 SSD 下使用 BitLocker 的论文
https://github.com/magnumripper/JohnTheRipper 已知密文的情况下尝试破解出明文的破解密码软件
https://github.com/shinnok/johnny JohnTheRipper 密码破解的 GUI 界面，理论兼容所有功能，有 windows 界面
https://github.com/jmk-foofus/medusa 支持的协议会比 hydra 少一点，但是某些速度会快
https://github.com/MrSqar-Ye/wpCrack wordpress hash 破解
https://github.com/testsecer/Md5Decrypt C#,基于网上 web API 的 MD5 搜索工具
https://github.com/s0md3v/Hash-Buster 能调用多个 API 进行 hash 破解查询的智能工具
https://www.52pojie.cn/thread-275945-1-1.html ARCHPR Pro4.54 绿色中文破解版。压缩包密码破解，利用“已知明文攻击”破解加密的压缩文件
```

网站管理与 Webshell

```
http://www.bt.cn 宝塔网站管理系统
https://github.com/AntSwordProject/antSword js,中国蚁剑,插件式开发
https://github.com/Chora10/Cknife java，中国菜刀
https://github.com/naozibuhao/SecQuanCknife java，中国菜刀升级版，增加爆破功能
https://github.com/euphrat1ca/hatchet 中国大砍刀
https://github.com/tengzhangchao/PyCmd py，一句话木马客户端程序，目前支持 php、jsp，CS 端通信加密
https://github.com/epinna/weevely3 py,利用特定的一句话脚本对网站进行管理
https://github.com/nil0x42/phpsploit py3,利用特定的一句话脚本对网站进行管理
https://github.com/wonderqs/Blade py，利用特定的一句话脚本对网站进行管理
https://github.com/anestisb/WeBaCoo perl，利用特定的一句话脚本对网站进行管理
https://github.com/keepwn/Altman .net 配合 mono，实现的跨平台菜刀
https://github.com/k4mpr3t/b4tm4n 集成伪造邮件 ddos，bat.php 的 webshell，初始 k4mpr3t
https://github.com/dotcppfile/DAws 过防火墙 webshell，post pass=DAws
https://github.com/b374k/b374k php 网站管理，默认密码 b374k
https://github.com/wso-shell/WSO webshell 的文件管理，可以伪装为 404 界面
https://github.com/UltimateHackers/nano php 小马，附带 py 编写的生成器
https://github.com/rebeyond/memShell 一款可以写入 java web server 内存中的 webshell
https://github.com/DXkite/freebuf-stream-shell PHP 使用流包装器实现 WebShell。freebuf 上有详细文章
https://xz.aliyun.com/t/2799 利用动态二进制加密实现新型一句话木马之客户端篇
https://github.com/rebeyond/Behinder “冰蝎”动态二进制加密网站管理客户端
https://xz.aliyun.com/t/2744#toc-8 利用动态二进制加密实现新型一句话木马之 Java 篇
https://xz.aliyun.com/t/2758#toc-4 利用动态二进制加密实现新型一句话木马之.NET 篇
https://xz.aliyun.com/t/2774#toc-4 利用动态二进制加密实现新型一句话木马之 PHP 篇
```

内网拓展后渗透

```
https://github.com/OpenWireSec/metasploit 后渗透框架
https://github.com/EmpireProject/Empire 基于 poweshell 的命令执行框架
https://github.com/TheSecondSun/Bashark 纯 Bash 脚本编写的后渗透框架，大鲨鱼
https://github.com/JusticeRage/FFM py3，拥有下载、上传功能，生成可执行 py 脚本的后门的后渗透框架
https://github.com/DarkSpiritz/DarkSpiritz py2,后渗透框架
https://github.com/byt3bl33d3r/CrackMapExec 网络测试中的瑞士军刀，包含 impacket、PowerSploit 等多种模块
https://github.com/SpiderLabs/scavenger 对 CrackMapExec 进行二次包装开发进行内网敏感信息扫描
https://github.com/jmortega/python-pentesting python-pentesting-tool python 安全工具相关功能模块
https://github.com/0xdea/tactical-exploitation Python/PowerShell 的测试脚本集
https://github.com/PowerShellMafia/PowerSploit powershell 测试脚本集与开发框架汇总
https://github.com/samratashok/nishang powershell 脚本集与利用框架
https://github.com/PowerShellEmpire/PowerTools PowerShell 脚本集，停止更新
https://github.com/FuzzySecurity/PowerShell-Suite PowerShell 脚本集
https://github.com/rvrsh3ll/Misc-Powershell-Scripts PowerShell 脚本集
https://github.com/nccgroup/redsnarf 窃取哈希，密码解密，偷偷调用猕猴桃等程序，rdp 多方法利用，远程启动 shell，清楚痕迹
https://github.com/BloodHoundAD/BloodHound 用于分析域成员和用用户关系的程序，通过用 powershell 脚本导出域内的 session、
computer、group、user 等信息，入库后进行可视化分析可以做到定点攻击。
https://github.com/xorrior/RemoteRecon 利用 DotNetToJScript 进行截图、key 记录、token 窃取、dll 与恶意代码注入
https://github.com/SkyLined/LocalNetworkScanner 利用浏览器漏洞当对方打开网址时，扫描对方内网信息
https://github.com/fdiskyou/hunter 调用 Windows API 对内网信息进行搜集很全面
https://github.com/0xwindows/VulScritp 内网渗透脚本，包括 banner 扫描、端口扫描；phpmyadmin、jenkins 等通用漏洞利用等
https://github.com/lcatro/network_backdoor_scanner 基于网络流量的内网探测框架
https://github.com/sowish/LNScan 详细的内部网络信息扫描器
https://github.com/rootlabs/nWatch 联动 nmap，并对组织内网进行扫描
https://github.com/m8r0wn/nullinux 用于 Linux 的内部渗透测试工具，可用于通过 SMB 枚举操作系统信息，域信息，共享，目录和用
户。
https://github.com/zMarch/Orc bash，Linux 下后渗透命令集合
```

远程控制 C2 服务器

```
https://github.com/malwaredllc/byob 僵尸网络生成框架
https://github.com/proxycannon/proxycannon-ng 构建攻击僵尸网络
https://github.com/deadPix3l/CryptSky/ 勒索软件 poc
https://github.com/jgamblin/Mirai-Source-Code 蠕虫病毒 poc
https://github.com/AhMyth/AhMyth-Android-RAT 基于 smali，Windows 下安卓远控，一对多带界面
https://github.com/ssooking/cobaltstrike3.12_cracked java1.8，远控、钓鱼、内网
https://github.com/Mr-Un1k0d3r/ThunderShell py2，CLI 与 web 端，内存马，RC4 加密 HTTP 传输
https://github.com/tiagorlampert/CHAOS go，win 远控，可过大部分杀软
https://github.com/Ne0nd0g/merlin go，c2 通讯，一对多
https://github.com/0x09AL/Browser-C2 go，利用 chrome 以浏览器的形式连接 C2 服务器
https://github.com/xdnice/PCShare c++，可以监视目标机器屏幕、注册表、文件系统等
https://github.com/quasar/QuasarRAT c#，一对多，界面
https://github.com/TheM4hd1/Vayne-RaT c#，一对多，界面
https://github.com/nettitude/PoshC2 PowerShell、C#，远控工具，有 win 提权组件
https://github.com/euphrat1ca/njRAT-v0.7d vb，常见蠕虫远控，有很多变种，一对多带界面
https://github.com/zerosum0x0/koadic py3,利用 JScript/VBScript 进行控制，大宝剑
https://github.com/Ridter/MyJSRat py2，利用 js 后门，配合 chm、hta 可实现很多后门方式。evi1cg.me/archives/chm_backdoor.html
https://github.com/its-a-feature/Apfell py3，macOS 与 linux 下的利用 js 后门，web 界面管理
https://github.com/peterpt/fuzzbunch py2，NSA 漏洞利用工具，配有自动化安装脚本与 gui 界面，远控 rat
https://github.com/n1nj4sec/pupy py，Windows，Linux，OSX，Android 跨平台，一对多
https://github.com/nathanlopez/Stitch py，Windows、Mac OSX、Linux 跨平台
https://github.com/neoneggplant/EggShell py，macos/osx 远控,可生成 HID 代码，一对多
https://github.com/Marten4n6/EvilOSX py，macos/osx 远控，一对多
https://github.com/vesche/basicRAT py3，simple 远控，一对多
https://github.com/Viralmaniar/Powershell-RAT py，截图通过 gmail 传输
https://github.com/byt3bl33d3r/gcat py，使用 gmail 作为 C&C 服务器
https://github.com/sweetsoftware/Ares py，c2 通讯，支持代理
https://github.com/micle-fm/Parat py，利用 telegram，windows 下的远程控制工具
https://github.com/ahhh/Reverse_DNS_Shell py，通过 dns 传输
https://github.com/iagox86/dnscat2 服务端为 ruby（linux），客户端为 C（win/linux），利用 DNS 协议进行端对端传输
https://github.com/deepzec/Grok-backdoor py，利用 ngrok 的后门
https://github.com/trustedsec/trevorc2 py，搭建一个合法的网站（可浏览），用于隐藏命令执行的客户端/服务器通信
```

端口转发与代理工具

```
https://github.com/fatedier/frp 用于内网穿透的高性能的反向代理应用，支持 tcp，udp，http，https 协议
https://github.com/inconshreveable/ngrok 端口转发，正反向代理，内网穿透
http://ngrok.ciqiuwl.cn/ 在线小米球 ngrok
https://github.com/knownsec/rtcp Socket 端口转发，用于远程维护
https://github.com/davrodpin/mole 基于 ssh 的端口转发
http://rootkiter.com/EarthWorm 一款用于开启 SOCKS v5 代理服务的工具，基于标准 C 开发，可提供多平台间的转接通讯，用于复杂网络环境下的数据转发。
http://rootkiter.com/Termite/README.txt EarthWorm 升级版，可以实现多节点跳跃
https://github.com/SECFORCE/Tunna 可以通过 HTTP 封装隧道通信任何 TCP，以及用于绕过防火墙环境中的网络限制
https://github.com/fbkcs/thunderdns 将 tcp 流量通过 DNS 协议转发，不需要客户端和 socket5 支持
https://github.com/sensepost/reGeorg reDuh 的升级版，主要是把内网服务器的端口通过 http/https 隧道转发到本机，形成一个回路。用于目标服务器在内网或做了端口策略的情况下连接目标服务器内部开放端口（提供了 php，asp，jsp 脚本的正反向代理）
https://github.com/SpiderClub/haipproxy py3,Scrapy and Redis,高可用 ip 代理池
https://github.com/chenjiandongx/async-proxy-pool py3 异步爬虫 ip 代理池
https://github.com/audibleblink/doxycannon 使用一个 openvpn 代理池，为每一个生成 docker，当连接某一个 vpn 后，其它的进行 socks5 转发做流量分发
https://github.com/decoder-it/psportfwd PowerShell 编写的端口转发工具，无需 admin 权限
https://github.com/ls0f/gortcp go，通过主控端、中转、被控端实现内网穿透
```

Cross 超越边界 NPV

```
https://github.com/bannedbook/fanqiang/wiki cross 汇总
https://github.com/teddysun/across 梯子搭建
https://github.com/ToyoDAdoubi/doubi 各种常用一键脚本
https://github.com/Nyr/openvpn-install openvpn 一键
https://github.com/quericy/one-key-ikev2-vpn CentOS/Debian/Ubuntu 一键安装 IPSEC/IKEV2 VPN 脚本
https://github.com/teddysun/shadowsocks_install shadowsocks,shadowsocksr
https://github.com/guyingbo/shadowproxy ss/socks5/http//https 等多种代理
https://github.com/shadowsocks/shadowsocks-manager shadowsocks 多用户管理
https://github.com/leitbogioro/SSR.Go shadowsocksrr 配置管理简化工具
https://github.com/ssrpanel/SSRPanel ss\ssr\v2ray 用户分布式管理
https://github.com/xuanhuan/ss-panel ss 用户分布式管理
https://github.com/Ahref-Group/SS-Panel-smarty-Edition ss 用户分布式管理，兑换码功能、商城系统，服务器信息
https://github.com/Ccapton/brook-web brook 程序服务端 Web 后台管理服务器（Linux|MacOS），基于 python、flask、flask-restful
https://github.com/Ccapton/brook-ok Brook 一键安装脚本
https://github.com/txthinking/brook go，支持 Linux/MacOS/Windows/Android/iOS 的代理与 vpn
https://github.com/gwuhaolin/lightsocks 轻量级网络混淆代理，基于 SOCKS5 协议，类 SS
https://github.com/Umbrellazc/BypassCampusNet 校园网防断网；UDP 53 免流上网
https://doub.io/dbrj-5/ 通过虚拟网卡转为类 VPN 全局代理 SSTAP，还有 sockscap64，比 proxifier 使用简单
https://github.com/ntkernel/lantern unlimited-landeng-for-win，无限流量蓝灯
https://www.psiphon3.com 开源赛风超越边界代理
https://hide.me 可试用
https://windscribe.com 可试用
http://www.vpngate.net 日本国立筑波大学超越边界代理
https://rava.app 注册可免费用一天
```

横向移动与密码 Hash 窃取

```
http://www.oxid.it/cain.html Cain & Abel 支持密码还原、arp 中间人攻击
https://github.com/gentilkiwi/mimikatz Windows 下以抓取密码为主的横向移动神器
https://github.com/skelsec/pypykatz 使用纯 py3 实现的 mimikatz
https://github.com/eladshamir/Internal-Monologue 无需 LSASS 进程使用 Mimikatz 从 LSASS 进程内存中提取内容，从内存中提取明文密码，NTLM 哈希，Kerberos ticket，以及执行 pass-the-hash/pass-the-ticket 攻击等
https://github.com/AlessandroZ/LaZagne py3，密码抓取工具
https://github.com/AlessandroZ/LaZagneForensic LaZagne 密码破解升级版，利用 DPAPI，目前缺陷是需要 windows user 密码
https://github.com/twelvesec/passcat Windows 下密码抓取工具
https://github.com/huntergregal/mimipenguin linux 密码抓取神器
https://github.com/quarkslab/quarkspwdump quarkslab 出品的密码抓取工具，不用注入任何进程
https://github.com/mthbernardes/sshLooter 从 ssh 服务中窃取用户名密码
https://github.com/nettitude/Invoke-PowerThIEf 利用 IE 进行后渗透，抓取密码、重定向等
https://github.com/GhostPack/Rubeus 操作 Kerberos 的库，实现了 Kekeo 的大部分功能，C#编写
https://github.com/m8r0wn/ldap_search PY,通过 ldap（轻量目录访问协议）认证，列举 win 域信息，爆破登录
```

Linux 提权相关

```
https://github.com/AlessandroZ/BeRoot py,通过检查常见的错误配置来查找提权方法. 支持 Windows/Linux/Mac
https://github.com/mschwager/0wned 利用 python 包进行高权限用户创建
https://github.com/mzet-/linux-exploit-suggester 查找 linux 有哪些补丁没有打的脚本
https://github.com/belane/linux-soft-exploit-suggester 查找 linux 有哪些有漏洞的软件
https://github.com/dirtycow/dirtycow.github.io 脏牛提权漏洞 exp
https://github.com/FireFart/dirtycow 脏牛提权漏洞 exp
https://github.com/stanleyb0y/sushell 利用 su 小偷实现低权限用户窃取 root 用户口令
https://github.com/jas502n/CVE-2018-17182/ Linux 内核 VMA-UAF 提权漏洞 CVE-2018-17182
https://github.com/jas502n/CVE-2018-14665 CVE-2018-14665，linux 下 Xorg X 服务器提权利用
https://github.com/nmulasmajic/syscall_exploit_CVE-2018-8897 Linux 系统利用 Syscall 实现提权
https://github.com/can1357/CVE-2018-8897 Linux 系统利用 Syscall 实现提权
https://github.com/SecWiki/linux-kernel-exploits linux-kernel-exploits Linux 平台提权漏洞集合
https://github.com/nilotpalbiswas/Auto-Root-Exploit linux 自动提权脚本
https://github.com/WazeHell/PE-Linux Linux 提权工具
https://guif.re/linuxeop linux 提权命令集合
```

Windows 提权相关

```
http://www.fuzzysecurity.com/tutorials/16.html windows 平台教程级提权参考文章
https://github.com/SecWiki/windows-kernel-exploits Windows 平台提权漏洞 Exp 集合
https://github.com/51x/WHP windows 下各种提权与利用工具
https://github.com/rasta-mouse/Sherlock win 提权漏洞验证
https://github.com/WindowsExploits/Exploits 微软 CVE-2012-0217、CVE-2016-3309、CVE-2016-3371、CVE-2016-7255、CVE-2017-0213 提权利用
https://github.com/decoder-it/lonelypotato RottenPotatoNG 变种，利用 NBNS 本地域名欺骗和 WPAD 代理欺骗提权
https://github.com/ohpe/juicy-potato RottenPotatoNG 变种，利用 com 对象、用户 token 进行提权
https://github.com/foxglovesec/Potato RottenPotatoNG 变种，利用本地域名欺骗和代理欺骗提权
https://github.com/DanMcInerney/icebreaker 处于内网环境但又在 AD 环境之外，icebreaker 将会帮助你获取明文 Active Directory 凭据（活动目录存储在域控服务器可用于提权）
https://github.com/hausec/ADAPE-Script Active Directory 权限提升脚本
https://github.com/klionsec/BypassAV-AllThings 利用 aspx 一句话配合提权 payload 提权
https://github.com/St0rn/Windows-10-Exploit msf 插件，win10 uac bypass
https://github.com/sam-b/CVE-2014-4113 利用 Win32k.sys 内核漏洞进行提取，ms14-058
https://github.com/breenmachine/RottenPotatoNG 利用 NBNS 本地域名欺骗和 WPAD 代理欺骗提权
https://github.com/unamer/CVE-2018-8120 影响 Win32k 组件，针对 win7 和 win2008 提权
https://github.com/alpha1ab/CVE-2018-8120 在 win7 与 win2k8 的基础上增加了 winXP 与 win2k3
https://github.com/0xbadjuju/Tokenvator 使用 Windows 令牌提升权限的工具，提供一个交互命令行界面
```

权限绕过

```
https://payloads.online/archivers/2018-12-22/1 DLL Hijacking & COM Hijacking ByPass UAC – 议题解读
https://github.com/tyranid/DotNetToJScript 能够利用 JS/Vbs 脚本加载.Net 程序的工具
https://github.com/mdsecactivebreach/SharpPack 绕过系统应用白名单执行 DotNet and PowerShell tools
https://github.com/rootm0s/WinPwnage py2，win 下权限提升，uac 绕过，dll 注入等
https://github.com/hfiref0x/UACME 包含许多用于多个版本操作系统上绕过 Windows 用户帐户控制的方法
https://github.com/Ben0xA/nps 实现了不使用 powershell.exe 的情况下执行 powershell 命令
https://github.com/Mr-Un1k0d3r/PowerLessShell 实现了不调用 powershell.exe 的情况下执行 powershell 命令
https://github.com/p3nt4/PowerShdll 使用 rundll32 运行 PowerShell，绕过软件限制
https://github.com/ionescu007/r0ak 内核层的瑞士军刀. 在 Windows10 内核中读/写/执行代码
https://github.com/leechristensen/UnmanagedPowerShell 从一个非托管程序来执行 PowerShell,经过一些修改后可以被用来注入到其他进程
https://github.com/stephenfewer/ReflectiveDLLInjection 一种库注入技术，让 DLL 自身不使用 LoadLibraryA 函数,将自身映射到目标进程内存中
https://github.com/ChrisAD/ads-payload 利用环境变量与 destop.ini 绕过 windows 下的 Palo Alto Traps endpoint 防护软件
https://github.com/Zer0Mem0ry/RunPE 通过内存读取，网络传输内容，利用 PE 执行 shellcode
```

沙盒逃逸

```
https://github.com/hacksysteam/WpadEscape 利用 wpad 进行浏览器 sandbox 沙箱逃逸
https://github.com/unamer/vmware_escape vmware 虚拟机逃逸。CVE-2017-4901，CVE-2018-6981，CVE-2018-6982
https://github.com/MorteNoir1/virtualbox_e1000_0day VirtualBox E1000 Guest-to-Host Escape 逃逸。教程
https://bugs.chromium.org/p/project-zero/issues/detail?id=1682&desc=2 Ghostscript：基于漏洞 CVE-2018-17961 的-dSAFER 沙盒逃逸技术
```

后门免杀代码混淆

```
https://www.shellterproject.com 杀毒软件绕过
https://github.com/trustedsec/unicorn py，一键生成多种后门
https://github.com/islamTaha12/Python-Rootkit windows 下 rootkit，反弹 meterpreter
https://github.com/n00py/Hwacha linux 下快速生成 metepreter 等多种 payload
https://github.com/Screetsec/Vegile msf 免杀，程序注入
https://github.com/MohamedNourTN/Terminator py2，msf 免杀
https://github.com/Veil-Framework/Veil msf 免杀
https://github.com/abedalqaderswedan1/aswcrypter py、bash，msf 免杀
https://github.com/Screetsec/TheFatRat java，msf 免杀，利用 searchsploit 快速搜索
https://github.com/pasahitz/zirikatu msf 免杀
https://github.com/govolution/avet msf 免杀
https://github.com/GreatSCT/GreatSCT msf 免杀
https://github.com/EgeBalci/HERCULES msf 免杀
https://github.com/trustedsec/nps_payload msf 免杀
https://github.com/4w4k3/Insanity-Framework py，payload 生成，过杀软，识别虚拟机，钓鱼，内存注入等
https://github.com/hlldz/SpookFlare Meterpreter，Empire，Koadic 等 loader/dropper 的生成器，可以绕过客户端检测和网络端检测的端点策略
https://github.com/pasahitz/regsvr32 使用 C#+Empire 实现最小体积免杀后门
https://github.com/malcomvetter/UnstoppableService 将自身安装为 Windows 服务且管理员无法停止/暂停服务的程序. C#编写
https://github.com/Cn33liz/StarFighters 基于 DotNetToJScript，利用 JavaScript 和 VBScript 执行 Empire Launcher
https://github.com/mdsecactivebreach/SharpShooter 基于 DotNetToJScript 使用 js、vbs，用于检索和执行任意 CSharp 源码的 payload 创建框架
https://github.com/mdsecactivebreach/CACTUSTORCH 基于 DotNetToJScript 使用 js、vbs 生成恶意 payload
https://github.com/OmerYa/Invisi-Shell 对 powershell 文件进行混淆
https://github.com/danielbohannon/Invoke-DOSfuscation 对 powershell 文件进行混淆，加密操作以及重新编码
https://github.com/danielbohannon/Invoke-Obfuscation 对 powershell 文件进行混淆，加密操作以及重新编码
https://github.com/Mr-Un1k0d3r/SCT-obfuscator Cobalt Strike SCT 有效载荷混淆器
https://github.com/tokyoneon/Armor bash，生成加密 Payload 在 macOS 上反弹 Shell
https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator 宏混淆，其中还包括 AV/Sandboxes 逃避机制
https://github.com/Kkevsterrr/backdoorme py3、py2 多种类型的后门、shell 生成工具，可以自动维持权限
https://github.com/TestingPens/MalwarePersistenceScripts win 下权限维持脚本
https://github.com/mhaskar/Linux-Root-Kit py，simple，linux 下 rootkit
https://github.com/PinkP4nther/Sutekh simple，rootkit，使普通用户获取 root shell
https://github.com/threatexpress/metatwin 从一个文件中提取元数据，包括数字签名，并注入到另一个文件中
https://github.com/Mr-Un1k0d3r/Windows-SignedBinary 可以修改二进制文件的 HASH，同时保留微软 windows 的签名
https://github.com/secretsquirrel/SigThief py，用于劫持合法的数字签名并绕过 Windows 的哈希验证机制的脚本工具
https://github.com/9aylas/Shortcut-Payload-Generator 快捷方式(.lnk)文件 Payload 生成器.AutoIt 编写
https://github.com/GuestGuri/Rootkit 反弹一个 tcp 连接，将进程 id 绑定到一个空文件夹
https://github.com/secretsquirrel/the-backdoor-factory 可以生成 win32PE 后门测试程序,ELF 文件后门程序等
```

文件捆绑

```
bat2exe.net 相类似也可以利用 iexpress 与 winrar 生成自解压 exe 可执行文件
https://github.com/islamadel/bat2exe 将 bat 文件转换为 exe 二进制文件
https://github.com/tywali/Bat2ExeConverter 将 bat 文件转换为 exe 二进制文件
https://github.com/Juntalis/win32-bat2exe 将 bat 文件转换为 exe 二进制文件
http://www.f2ko.de/downloads/Bat_To_Exe_Converter.zip 将 bat 文件转换为 exe 二进制文件，可以隐藏窗口。
https://github.com/r00t-3xp10it/trojanizer 将两个可执行文件打包为自解压文件，自解压文件在执行时会执行可执行文件
https://github.com/r00t-3xp10it/backdoorppt 将 payload 更换图标
https://github.com/r00t-3xp10it/FakeImageExploiter 将 payload 更换图标。需要 wine 与 resourcehacker 环境
https://github.com/DamonMohammadbagher/FakeFileMaker 更换图标和名称
https://github.com/peewpw/Invoke-PSImage 将 PS 脚本隐藏进 PNG 像素中并用一行指令去执行它
https://github.com/Mr-Un1k0d3r/DKMC Don’t kill my cat 生成混淆的 shellcode，将 shellcode 存储在多语言图像中
https://github.com/deepzec/Bad-Pdf 生成一个 pdf 文件，内含 payload 来窃取 win 上的 Net-NTLM 哈希
https://github.com/3gstudent/Worse-PDF 向 PDF 文件中插入恶意代码，来窃取 win 上的 Net-NTLM 哈希
```

社工相关

```
https://github.com/brannondorsey/PassGAN py,深度学习,密码字典样本生成
https://github.com/Mebus/cupp 根据用户习惯密码生成弱口令探测
https://github.com/Saferman/cupper 根据用户习惯密码生成弱口令探测，楼上升级
https://github.com/LandGrey/pydictor py3，特定密码字典生成
https://github.com/mehulj94/Radium-Keylogger python 下的键盘记录工具
https://github.com/threatexpress/domainhunter 检查过期域名，bluecoat 分类和 Archive.org 历史记录，以确定最为适合于钓鱼和 C2 的域名
https://github.com/Mr-Un1k0d3r/CatMyPhish 收集目标类似的尚未注册的域名
https://github.com/x0day/Multisearch-v2 Bing、google、360、zoomeye 等搜索引擎聚合搜索，可用于发现企业被搜索引擎收录的敏感资产信息
https://github.com/n0tr00t/Sreg Sreg 可对使用者通过输入 email、phone、username 的返回用户注册的所有互联网护照信息。
https://github.com/SpiderLabs/social_mapper 社交媒体枚举和关联工具，通过人脸识别关联人物侧写
https://github.com/vysec/MaiInt 公司雇员信息收集测试工具
https://github.com/jofpin/trape py，利用 OSINT 对人员进行追踪定位
https://github.com/famavott/osint-scraper 输入人名或邮箱地址，自动从互联网爬取关于此人的信息
https://github.com/xHak9x/fbi py2,facebook 脸书信息搜集工具
https://github.com/initstring/linkedin2username 通过 Linkedin 领英获取相关公司员工列表
https://github.com/0x09AL/raven linux 下领英 Linkedin information gathering tool
https://github.com/Ridter/Mailget 通过脉脉用户猜测企业邮箱
https://github.com/haccer/tweep 使用 twitter API 进行信息爬取查询
https://github.com/MazenElzanaty/TwLocation py，获取 Twitter 用户发推的地址
https://github.com/vaguileradiaz/tinfoleak web 界面，对某人的 twitter 进行全面的情报分析
https://github.com/deepfakes 虚假音视频制作
https://www.jianshu.com/p/147cf5414851 聊聊那些常见的探侦类 APP
https://github.com/thinkst/canarytokens 重要文件的追踪溯源，信标定位（https://canarytokens.org/generate#）
https://github.com/ggerganov/kbd-audio c++,linux,利用麦克风监控键盘输入测试输入值
```

钓鱼框架邮件伪造

https://github.com/bhdresh/SocialEngineeringPayloads 负责收集用于证书盗窃和鱼叉式网络钓鱼攻击的社交工程技巧和 payloads
https://github.com/trustedsec/social-engineer-toolkit 专为社交工程设计的开源渗透测试框架
https://github.com/thelinuxchoice/blackeye 拥有 facebook、instagram 等三十余个钓鱼模板的一键启用工具
https://github.com/M4cs/BlackEye-Python 以 blackeye 为基础加强子域的管理
https://github.com/azizaltuntas/Camelishing py3，界面化社会工程学攻击辅助工具
https://github.com/JonCooperWorks/judas go，克隆网站钓鱼
https://github.com/gophish/gophish go，拥有在线模板设计、发送诱骗广告等功能的钓鱼系统
https://github.com/tatanus/SPF py2，deefcon 上的钓鱼系统
https://github.com/MSG-maniac/mail_fishing 甲方内部钓鱼系统
https://github.com/samyoyo/weeman 钓鱼的 http 服务器
https://github.com/Raikia/FiercePhish 可以管理所有钓鱼攻击的完整钓鱼框架，允许你跟踪单独的网络钓鱼活动，定时发送电子邮件等
https://github.com/securestate/king-phisher 可视化钓鱼活动工具包
https://github.com/fireeye/ReelPhish 实时双因素网络钓鱼工具
https://github.com/kgretzky/evilginx 绕过双因素验证的钓鱼框架
https://github.com/kgretzky/evilginx2 MiTM 框架，登录页面钓鱼，绕过双因素认证等
https://github.com/ustayready/CredSniper 使用 Flask 和 Jinja2 模板编写的网络钓鱼框架，支持捕获 2FA 令牌
https://github.com/fireeye/PwnAuth OAuth 滥用测试检测平台
https://github.com/n0pe-sled/Postfix-Server-Setup 自动化建立一个网络钓鱼服务器
https://github.com/Dionach/PhEmail py2，钓鱼与邮件伪造
https://github.com/PHPMailer/PHPMailer 世界上最流行的 PHP 发送邮件的代码
http://tool.chacuo.net/mailanonymous 在线邮件伪造
http://ns4gov.000webhostapp.com 在线邮件伪造

中间人攻击流量劫持

https://github.com/bettercap/bettercap 网络攻击以及监控的瑞士军刀。该工具支持多种模块，比如 ARP/DNS 欺骗、TCP 以及数据包代理等
https://github.com/mitmproxy/mitmproxy PY,支持 SSL 拦截，进行 https 流量代理
https://github.com/qiyeboy/BaseProxy py3,异步 http/https 代理,楼上简化版。可以作为中间人工具，比如说替换网址图片等
https://github.com/lgandx/Responder 用于嗅探网络内所有的 NTLM、NTLMv1/v2、Net-NTLMv1/v2 包，对网络内主机进行欺骗获取用户 hash。a 拿着 b 密码请求 b，c 对 a 说我是 b，然后 c 获得了 b 的密码，https://www.secpulse.com/archives/65503.html 【脉搏译文系列】渗透师指南之 Responder。
https://github.com/Kevin-Robertson/Inveigh 一款 PowerShell LLMNR / mDNS / NBNS 欺骗器和中间人工具
https://github.com/LionSec/xerosploit 中间人攻击测试工具包
https://github.com/AlsidOfficial/WSUSpendu 可以自主创建恶意更新，并将其注入到 WSUS 服务器数据库中，然后随意的分发这些恶意更新
https://github.com/infobyte/evilgrade 一个模块化的脚本框架，使攻击者在不知情的情况下将恶意更新注入到用户更新中
https://github.com/quickbreach/smbetray 专注于通过文件内容交换、lnk 交换来攻击客户端，以及窃取任何以明文形式传输的数据
https://github.com/mrexodia/haxxmap 对 IMAP 服务器进行中间人攻击

协议解析流量还原分析

https://github.com/wireshark/wireshark 协议解析流量分析还原
https://github.com/CoreSecurity/impacket Impacket 是用于处理网络协议的 Python 工具包集合，内网中可用以提权例如 wmiexec.py、NMB，SMB1-3 和 MS-DCERPC 提供对协议实现本身的低级别编程访问。
https://github.com/secdev/scapy 内置了交互式网络数据包处理、数据包生成器、网络扫描器网络发现和包嗅探工具，提供多种协议包生成及解析插件，能够灵活的的生成协议数据包，并进行修改、解析。
https://gitee.com/qielige/openQPA 协议分析软件 QPA 的开源代码，特点是进程抓包、特征自动分析
https://github.com/jtpereyda/boofuzz 网络协议 fuzz 测试
https://www.jianshu.com/p/4dca12a35158 5 个常用的免费报文库
https://github.com/zerbea/hcxdumptool 从 Wlan 设备上捕获数据包
https://github.com/NytroRST/NetRipper 支持截获像 putty,winscp,mssql,chrome,firefox,outlook，https 中的明文密码
https://github.com/shramos/polymorph 支持几乎所有现有协议的实时网络数据包操作框架
https://github.com/nospaceships/raw-socket-sniffer C,PS，无需驱动抓取 Windows 流量

无线网络 WIFI 中间人攻击

```
https://github.com/wi-fi-analyzer/fluxion 窃取用户 wifi 密码的进行密码重放攻击
https://github.com/0v3rl0w/e013 窃取 Wifi 密码. VB 脚本
https://github.com/cls1991/ng 获取你当前连接 wifi 的密码与 ip
https://github.com/wifiphisher/wifiphisher PY,中间人攻击，FakeAp 恶意热点，WIFI 钓鱼，凭证窃取
https://github.com/1N3/PRISM-AP 自动部署 RogueAP(恶意热点) MITM 攻击框架
https://github.com/sensepost/mana Wifi 劫持工具，可以监听计算机或其他移动设备的 Wifi 通信，并能够模仿该设备
https://github.com/deltaxflux/fluxion bash 与 py，对使用 wpa 协议的无线网络进行 MiTM 攻击
https://github.com/DanMcInerney/LANs.py ARP 欺骗，无线网络劫持
```

无线网络 WIFI 防御

```
https://github.com/SYWorks/waidps PY,Linux 下无线网络入侵检测工具
https://github.com/SkypLabs/probequest 嗅探和显示无线网卡附近的 Wifi Probe 请求
https://github.com/wangshub/hmpa-pi 在树莓派或路由，利用 Wireshark 扫描附近网络 WiFi 设备，当有手机或其它 Wi-Fi 设备在附近时，通过邮件或者微信提醒
https://github.com/besimaltnok/PiFinger 检查 wifi 是否为”Wifi-Pineapple 大菠萝”所开放的恶意热点
https://github.com/WiPi-Hunter/PiSavar 利用 PineAP，对于 FAKE AP 虚假接入点，如”Wifi-Pineapple 大菠萝”进行监测
```

无线网络 WIFI 审计测试

```
https://www.wifislax.com 西班牙 wifi 审计系统，国内汉化版为无线革新 5.1.1 Wifislax-WRC
https://cn.elcomsoft.com/ewsa.html ewsa，wifi 嗅探，握手包密码还原，EWSA-173-HC1UW-L3EGT-FFJ3O-SOQB3
https://www.passcape.com wifipr，握手包密码还原，另外还有许多商业版 windows 下密码还原工具
https://github.com/MisterBianco/BoopSuite 无线网络审计工具，支持 2-5GHZ 频段
https://github.com/aircrack-ng/aircrack-ng 由数据包嗅探器、检测器、WPA / WPA2-PSK 解密器、WEP 和用于 802.11 无线局域网的分析工具组成
https://github.com/t6x/reaver-wps-fork-t6x wps 跑 pin 码攻击，常见 wifi 攻击
https://github.com/derv82/wifite2 wifite 无线审计工具升级版，联动 aircrack-ng 与 reaver
https://github.com/savio-code/fern-wifi-cracker 无线安全审计工具
https://github.com/P0cL4bs/WiFi-Pumpkin 无线安全渗透测试套件
https://github.com/entropy1337/infernal-twin 自动化无线攻击工具 Infernal-Wireless
https://github.com/m4n3dw0lf/PytheM Python 网络/渗透测试工具
https://github.com/InfamousSYN/rogue 无线网络攻击工具包
https://github.com/cSploit/android 手机 WiFi 渗透工具框架，可以使用 msf
https://github.com/chrisk44/Hijacker 手机 wifi 测试工具
https://andrax-pentest.org/ kali hunter 手机渗透测试系统
https://www.zimperium.com/zanti-mobile-penetration-testing 手机 wifi 渗透工具
```

数据取回隐秘传输

```
https://github.com/TryCatchHCF/Cloakify 躲避 DLP/MLS 数据泄露防护系统，突破数据白名单控制，躲避 AV 检测进行数据盗取
https://github.com/sensepost/DET 使用单个或多个通道同时执行数据取回
https://github.com/Arno0x/DNSExfiltrator 利用 DNS 解析进行数据隐秘传输的工具
https://github.com/ytisf/PyExfil 用于数据取回的 Python 软件包
https://github.com/Arno0x/ReflectiveDnsExfiltrator 反射 DNS 解析隐蔽通道进行数据泄露
```

硬件安全

```
https://github.com/unprovable/PentestHardware 硬件渗透测试实用手册
https://ducktoolkit.com/ 橡皮鸭、HID 键盘模拟器
https://github.com/insecurityofthings/jackit 用于 Mousejack 的开发代码
https://github.com/samyk/magspoof 信用卡信息盗取
https://github.com/mame82/P4wnP1_aloa 在树莓派 Raspberry Pi 上安装常用的测试组件，打造移动测试平台
https://www.freebuf.com/geek/195631.html 成为物理黑客吧！利用树莓派实现 P4wnP1 项目进行渗透测试
https://github.com/mame82/P4wnP1 在树莓派安装网络劫持键盘注入(WHID)工具
https://github.com/ebursztein/malusb 创建跨平台的 HID 欺骗 payload，并在 Windows 和 OSX 上建立反向 TCP-shell
https://github.com/Orange-Cyberdefense/fenrir-ocd 主要功能和用途是绕过有线 802.1x 保护并使你能够访问目标网络
https://github.com/360PegasusTeam/GhostTunnel 可在隔离环境下使用 HID 生成隐蔽后门，释放有效负载后删除自身
https://github.com/LennyLeng/RadioEye RFID 配合常见的 NFC 使用
https://github.com/Proxmark/proxmark3/ RFID 神器 PM3
http://www.freebuf.com/news/others/605.html RFID Hacking-资源大合集
https://github.com/UnicornTeam/HackCube-Special 独角兽实验室硬件渗透测试平台
```

IoT 安全

```
https://github.com/w3h/icsmaster 整合工控安全资源
https://github.com/V33RU/IoTSecurity101 IoT 工控安全与物联网安全学习的一些文章和资源
http://www.freebuf.com/ics-articles 工控相关
http://www.freebuf.com/sectool/174567.html 工业控制系统（ICS）安全专家必备的测试工具和安全资源
http://www.freebuf.com/articles/ics-articles/178822.html 浅析煤炭企业如何进行工控安全建设
http://www.freebuf.com/articles/network/178251.html 工控安全现场实施经验谈之工控系统如何加强主机防护
https://github.com/hslatman/awesome-industrial-control-system-security 工控系统安全方向优秀资源收集仓库
https://github.com/adi0x90/attifyos IoT 集成安全测试系统，带有一些常用的软件
https://github.com/moki-ics/moki 一键配置类似 kali 的工控渗透测试系统的脚本，
https://gitlab.com/expliot_framework/expliot py3，工控安全漏洞测试框架
https://github.com/dark-lbp/isf py2,工控中类似 msf 的测试框架
https://github.com/enddo/smod py2，使用了 scapy 模块，主要针对 modbus 协议测试
https://github.com/shodan-labs/iotdb nmap 配合 shodan API 扫描 IoT 设备
https://github.com/XHermitOne/icscanner 带界面的 ics 扫描器
https://github.com/yanlinlin82/plcscan 通过 TCP/102 和 TCP/502 识别互联网上 PLC 设备和其他 Modbus 设备
https://github.com/nsacyber/GRASSMARLIN NSA 旗下 ICS/SCADA 态势感知
https://github.com/nezza/scada-stuff 对 SCADA/ICS 设备进行逆向与攻击
```

摄像头安全

```
https://github.com/woj-ciech/kamerka 配合 shodan API 扫描到的摄像头地理位置显示在地图上
https://github.com/Ullaakut/cameradar GO,针对摄像头 RTSP 协议渗透测试，附弱口令字典
https://github.com/Ullaakut/camerattack GO,摄像头远程禁用
https://github.com/NIteshx2/UltimateSecurityCam py3，摄像头监测外来人员软件，有防欺骗设置
```

路由安全

```
http://stascorp.com RouterScan 毛子开发的路由器漏洞利用工具，界面化很强大
https://github.com/threat9/routersploit py3，仿 msf 路由器漏洞利用框架
https://github.com/jh00nbr/Routerhunter-2.0 已停止更新，路由器漏洞扫描利用
https://github.com/googleinurl/RouterHunterBR php，路由器设备漏洞扫描利用
https://github.com/scu-igroup/telnet-scanner Telnet 服务密码撞库
```

物联网安全

```
https://github.com/RUB-NDS/PRET 打印机攻击框架
https://github.com/rapid7/IoTSeeker 物联网设备默认密码扫描检测工具
https://github.com/schutzwerk/CANalyzat0r 专有汽车协议的安全分析工具包
https://github.com/pasta-auto 智能汽车测试
```

Fuzz 模糊测试漏洞挖掘

```
http://www.freebuf.com/articles/rookie/169413.html 一系列用于 Fuzzing 学习的资源汇总
https://github.com/secfigo/Awesome-Fuzzing Fuzz 相关学习资料
https://github.com/fuzzdb-project/fuzzdb fuzz 资料数据库
https://github.com/ivanfratric/winafl AFL for fuzzing Windows binaries,原创技术分析 | AFL 漏洞挖掘技术漫谈
https://github.com/attekett/NodeFuzz a fuzzer harness for web browsers and browser like applications.
https://github.com/google/oss-fuzz Continuous Fuzzing for Open Source Software
http://blog.topsec.com.cn/ad_lab/alphafuzzer/ 以文件格式为主的漏洞挖掘工具
https://bbs.ichunqiu.com/thread-24898-1-1.html Test404 -HTTP Fuzzer V3.0
https://github.com/xmendez/wfuzz py，Web 安全模糊测试工具，模块化可处理 burp 所抓请求和响应报文
https://github.com/1N3/BlackWidow 基于 Python 实现的 Web 爬虫，用于收集目标网站的情报信息并对 OWASP 漏洞进行模糊测试
https://github.com/bunzen/pySSDeep py，一个基于模糊哈希（Fuzzy Hashing）算法的工具。go，glaslos/ssdeep；C，ssdeep-project/ssdeep
https://github.com/googleprojectzero/winafl AFL 针对 Windows 二进制进行测试
```

安全防护

```
https://github.com/baidu/AdvBox Advbox 是支持多种深度学习平台的 AI 模型安全工具箱，既支持白盒和黑盒算法生成对抗样本，衡量 AI 模型鲁棒性，也支持常见的防御算法
https://github.com/quoscient/octopus 区块链智能合约安全分析工具
https://github.com/Cyb3rWard0g/HELK 具有高级分析功能的威胁狩猎 ELK
https://github.com/trimstray/otseca linux 系统审计工具，可以导出系统配置，生成报表
https://github.com/BugScanTeam/DNSLog 一款基于 django 监控 DNS 解析记录和 HTTP 访问记录的工具，可以配合盲注、xss、解析对方真实 ip 使用
https://github.com/mwrlabs/dref DNS 重绑定利用框架
https://github.com/chengr28/Pcap_DNSProxy/blob/master/README.zh-Hans.md Pcap_DNSProxy 是一个基于 WinPcap/LibPcap 用于过滤 DNS 投毒污染的工具
https://github.com/PlagueScanner/PlagueScanner 使用 python 实现的集成 ClamAV、ESET、Bitdefender 的反病毒引擎
https://github.com/m4rco-/dorothy2 一款木马、僵尸网络分析框架
http://github.com/jumpserver/jumpserver 基于 Python3 的开源堡垒机
https://github.com/github/glb-director 负载均衡组件 GLB，数据解析使用了 dpdk
https://github.com/processhacker/processhacker 监控系统资源、软件调试、检测恶意软件，管理进程
https://github.com/TKCERT/mail-security-tester 检测邮件防护与过滤系统的测试框架
https://github.com/chaitin/sqlchop-http-proxy 利用 HTTP 反向代理，内置 SQLChop 作为 SQL 注入攻击检测模块，可以拦截 SQL 注入流量而放行正常流量
https://github.com/OWASP/SecureTea-Project 当有人私自触碰电脑鼠标或触摸板，进行报警
```

代码审计应用测试

```
https://www.waitalone.cn/seay-source-code-auditv2.html Seay 源代码审计系统 2.1 版本
https://github.com/pyupio/safety 检查所有已安装 Python 包，查找已知的安全漏洞
https://github.com/pumasecurity/puma-scan 实时代码审计，vs 插件
https://github.com/wufeifei/cobra 白盒代码安全审计系统
https://github.com/OneSourceCat/phpvulhunter 静态 php 代码审计
https://github.com/ripsscanner/rips 基于 php 的 php 代码审计工具
https://github.com/Qihoo360/phptrace 跟踪、分析 PHP 运行情况的工具
https://github.com/ajinabraham/NodeJsScan Node.JS 应用代码审计
https://github.com/ctxis/beemka 针对 Electron App 的漏洞利用工具包
https://github.com/doyensec/electronegativity Electron 应用代码审计，App 的错误配置和安全问题
https://github.com/shengqi158/pyvulhunter Python 应用审计
https://github.com/securego/gosec Go 语言源码安全分析工具
https://github.com/GoSSIP-SJTU/TripleDoggy 基于 clang 的 c/c++/object-c 源代码检测框架，有大量接口可以被调用
https://github.com/ga0/pyprotect 给 python 代码加密，防止逆向
https://github.com/presidentbeef/brakeman Ruby on Rails 应用静态代码分析
https://github.com/python-security/pyt 用于检测 Python Web 应用程序中的安全漏洞的静态分析工具
https://github.com/m4ll0k/WPSploit WordPress 插件代码安全审计
https://github.com/elcodigok/wphardening 加强任何 WordPress 安装的安全
```

大数据平台安全

```
https://github.com/shouc/BDA 针对 hadoop/spark/mysql 等大数据平台的审计与检测
https://github.com/wavestone-cdt/hadoop-attack-library hadoop 测试方式和工具集
```

蜜罐安全

```
https://github.com/paralax/awesome-honeypots 蜜罐开源技术收集
https://github.com/threatstream/mhn 现代蜜网，集成了多种蜜罐的安装脚本，可以快速部署、使用，也能够快速的从节点收集数据
https://github.com/dtag-dev-sec/tpotce T-POT，里面使用 docker 技术实现多个蜜罐组合，配合 ELK 进行研究与数据捕获
https://www.freebuf.com/sectool/190840.html T-Pot 多蜜罐平台使用心法
https://github.com/n3uz/t-pot-autoinstall 将 fork 的 T-POT 蜜罐的一键安装脚本替换为国内加速镜像
```

Web 蜜罐内网监测

```
https://github.com/micheloosterhof/cowrie py2，使用 ELK（ElasticSearch，LogStash，Kibana）进行数据分析，目前支持 ssh，telnet，sftp 等协议
https://github.com/mushorg/snare py3，web 安全蜜罐，可克隆指定 Web 页面
https://github.com/honeynet/beeswarm py，使用 agent 探针与蜜罐进行实时交互来引诱攻击者
https://github.com/thinkst/opencanary PY2,SNMP\RDP\SAMBA 蜜罐
https://github.com/p1r06u3/opencanary_web PY,TORNADO,内网低交互蜜罐。支持自动化安装，目前支持常见的 16 中协议，现为探针/蜜罐-管理的架构，可以考虑二次开发为探针-沙盒-管理的架构
https://github.com/p1r06u3/opencanary_web
https://github.com/Cymmetria 知名欺骗防御蜜罐组织。Struct、weblogic、telnet、Cisco ASA、Micros 等仿真蜜罐
https://github.com/Cymmetria/honeycomb Cymmetria 公司开源蜜罐框架，低交互
https://github.com/honeytrap/honeytrap 可扩展蜜罐框架，支持探针部署与高交互蜜罐
https://gosecure.net/2018/12/19/rdp-man-in-the-middle-smile-youre-on-camera/ RDP MITM，打造可记录图像和按键的 RDP 蜜罐（https://github.com/gosecure/pyrdp）
```

摄像头蜜罐

```
https://github.com/alexbredo/honeypot-camera py，摄像头蜜罐。tornado 模拟 WEB 服务，图片代替视频，可以考虑后期多加点图片和按钮
https://github.com/EasyDarwin/EasyIPCamera C，RTSP 服务器组件用以构建摄像头蜜罐
```

工控蜜罐

```
https://github.com/sjhilt/GasPot 模拟油电燃气工控系统
https://github.com/djformby/GRFICS IoT 工业仿真系统模拟框架，采用 MODBUS 协议对 PLC 虚拟机监视和控制
https://github.com/RabitW/IoTSecurityNAT IoT 测试系统，方便快速接入各种设备，进行安全测试
https://github.com/mushorg/conpot 针对 ICS/SCADA 的低交互工控蜜罐，模拟 Modbus 和 S7comm
```

逆向相关

```
https://www.peerlyst.com/posts/resource-learning-how-to-reverse-malware-a-guide 恶意软件逆向指南和工具的集合
https://github.com/ReFirmLabs/binwalk 二进制 pwn 文件自动化逆向，拥有多种插件
https://github.com/angr/angr 一个具有动态符号执行和静态分析的二进制分析工具
https://github.com/endgameinc/xori 自定义反汇编框架
https://down.52pojie.cn/ 吾爱破解爱盘工具包
https://github.com/blacknbunny/peanalyzer32 PE 文件分析和反汇编工具
https://github.com/DominicBreuker/pspy 不用 root 权限就可以监控进程运行
```

CTF 相关

```
https://ctf-wiki.github.io/ctf-wiki/ CTFwiki，Misc/Crypto/Web/Assembly/Executable/Reverse/Pwn/Android/ICS
https://github.com/adon90/pentest_compilation ctf 比赛与 OSCP 考试中常见的知识点和命令
https://github.com/gabemarshall/microctfs 小型 ctf 镜像 docker
https://github.com/giantbranch/pwn_deploy_chroot 部署多个 pwn 题到一个 docker 容器中
https://github.com/facebook/fbctf CTF 比赛框架
https://github.com/0Chencc/CTFCrackTools CTF 工具集成包
https://github.com/guyoung/CaptfEncoder CTF 密码编码全家桶，还有小程序版本
https://github.com/Gallopsled/pwntools pwn 类型，二进制利用框架
https://github.com/ChrisTheCoolHut/Zeratool pwn 类型，二进制利用框架
https://github.com/ChrisTheCoolHut/Rocket-Shot pwn，自动攻击脚本
https://0xrick.github.io/lists/stego/ 隐写术工具集，Steganography – A list of useful tools and resources
https://github.com/DominicBreuker/stego-toolkit 隐写工具包
https://github.com/bugsafe/WeReport WeReport 报告助手
https://github.com/PELock/CrackMeZ3S-CTF-CrackMe-Tutorial 为 CTF 比赛编写 CrackMe 软件
```

计算机与移动设备取证调查

```
https://www.freebuf.com/articles/rookie/195107.html 记一次微信数据库解密过程。微信的加密数据库的解密密码是由“设备的 IMEI(MEID)+用户的 uin，进行 MD5，然后取其前 7 位小写字母”构成的
https://www.audacityteam.org/ 音频文件和波形图处理工具
http://www.sweetscape.com/010editor/ 识别不同文件格式（模板）的 16 进制编辑器，具有文件修复功能
http://www.magicexif.com/ 将照片图像中的 exif 信息数据化
http://mediaarea.net/MediaInfo 类似 exiftool 来查看内容区域和元数据信息
https://www.sno.phy.queensu.ca/~phil/exiftool/ 检查图像文件的 exif 元数据
https://www.gimp.org/ Gimp 提供了转换各类图像文件可视化数据的功能，还可以用于确认文件是否是一个图像文件
https://github.com/volatilityfoundation/volatility windows 内存取证分析
https://github.com/gleeda/memtriage Windows 内存取证分析
https://github.com/SekoiaLab/Fastir_Collector Windows 取证/信息收集，不限于内存，注册表，文件信息等
https://github.com/Viralmaniar/Remote-Desktop-Caching– RDP 信息复原，png 图片格式
https://github.com/comaeio/LiveCloudKd C，针对 Hyper-V 的内存取证
–https://github.com/sevagas/swap_digger 针对 Linux swap 进行取证分析的工具
http://extundelete.sourceforge.net/ linux 下的文件恢复
https://github.com/viaforensics/android-forensics 安卓取证 App 和框架，可以对安卓设备内各种信息进行提取
https://github.com/davidmcgrew/joy 用来捕获和分析内外网流量数据的包，主要用于进行网络调查、安全监控和取证
https://github.com/USArmyResearchLab/Dshell 可扩展的网络取证分析框架，支持快速开发插件与解析网络数据包捕获
http://qpdf.sourceforge.net/ 查看 pdf 文件并整理提取信息
http://zipinfo.com/ 在无需提取的情况下列出了 zip 文件的内容信息
http://f00l.de/pcapfix/ pcap 文件修复
https://www.cgsecurity.org/wiki/TestDisk 磁盘分区修复
https://github.com/decalage2/oletools py，用于分析 MS OLE2 文件（结构化存储，复合文件二进制格式）和 MS Office 文档
https://www.xplico.org/download 内存取证
https://github.com/google/bochspwn-reloaded Bochspwn Reloaded（内核信息泄漏检测）工具
https://github.com/abrignoni/DFIR-SQL-Query-Repo 收集用于数据取证的 SQL 查询模板
https://www.freebuf.com/news/193684.html iOS 取证技巧：在无损的情况下完整导出 SQLite 数据库
```

移动安全

```
https://github.com/Brucetg/App_Security App 安全学习资源
https://github.com/rovo89/Xposed 随心所欲修改安卓手机系统
https://github.com/android-hacker/VirtualXposed 基于 VirtualApp 和 epic 在非 ROOT 环境下运行 Xposed 模块的实现
https://github.com/MobSF/Mobile-Security-Framework-MobSF 移动安全审计框架。android、ios、win
https://github.com/WooyunDota/DroidSSLUnpinning 安卓证书锁定解除的工具
https://github.com/nccgroup/house 运行时手机 App 分析工具包，带 Web GUI
https://github.com/UltimateHackers/Diggy 从 Apk 文件中提取 URLs 的工具
https://github.com/nettitude/scrounger iOS 和 Android 移动应用程序渗透测试框架
https://github.com/XekriCorp/LeakVM 安卓应用安全测试框架
https://github.com/zsdlove/ApkVulCheck 安卓漏洞扫描工具
https://github.com/samyk/frisky 针对 ios/macOS 应用的嗅探/修改/逆向/注入等工具
https://github.com/GeoSn0w/OsirisJailbreak12 IOS12 不完全越狱
https://github.com/chaitin/passionfruit iOS 应用逆向与分析工具，可以大大加速 iOS 应用安全分析过程
```

防火墙规则、Waf、CDN 相关

```
https://github.com/baidu/openrasp RASP,Runtime Application Self-Protection，实时应用自我保护，更智能，针对每个语言定制
https://github.com/snort3/snort3 snort 算是最出名的开源 ids 入侵检测
https://github.com/chaitin/yanshi 长亭偃师（yanshi）,雷池（SafeLine）防火墙核心引擎使用到的代码生成工具
https://github.com/SpiderLabs/ModSecurity C，跨平台 WAF engine for Apache, IIS and Nginx
https://github.com/klaubert/waf-fle ModSecurity Web 控制台
https://github.com/xsec-lab/x-waf 适用于中小企业的云 waf
https://github.com/jx-sec/jxwaf 基于 openrestynginx+lua 开发，独创的业务逻辑防护引擎和机器学习引擎，解决传统 WAF 无法对业务安全进行防护的痛点
https://github.com/loveshell/ngx_lua_waf 基于 lua-nginx-moduleopenresty 的 web 应用防火墙
https://github.com/Janusec/janusec 基于 Golang 开发的应用安全网关，具备 WAF、CC 攻击防御、证书私钥加密、负载均衡、统一 Web 化管理等功能。
https://github.com/SpiderLabs/owasp-modsecurity-crs a set of generic attack detection rules for use with ModSecurity or compatible web application firewalls
https://github.com/kirillwow/ids_bypass IDS Bypass 脚本
https://github.com/milo2012/ipv4bypass 利用 ipV6 地址绕过 waf
https://github.com/3xp10it/bypass_waf 防火墙绕过脚本
https://github.com/m0rtem/CloudFail 针对 Cloudfail,查找位于 CDN 后面网站的真实 IP
https://github.com/Nitr4x/whichCDN CDN 识别、检测
https://github.com/3xp10it/xcdn 尝试找出 cdn 背后的真实 ip，3xp10it.github.io 博客
```

入侵检测

```
https://github.com/Neo23x0/Loki 一款 APT 入侵痕迹扫描器
https://github.com/ossec/ossec-hids 开源 hids 堡垒机
https://github.com/grayddq/HIDS hids 基于主机型入侵检测系统，一个人的安全部
https://github.com/ysrc/yulong-hids 驭龙 HIDS 是一款由 YSRC 开源的入侵检测系统
https://github.com/DianrongSecurity/AgentSmith-HIDS 点融开源 HIDS，开源部分为主机情报收集工具
https://github.com/Tencent/HaboMalHunter 哈勃分析系统，linux 系统病毒分析及安全测试
https://github.com/JPCERTCC/LogonTracer 根据 win 登陆记录日志来分析并用图形化展示恶意登陆行为
https://github.com/anwi-wips/anwi 无线 IDS，基于低成本的 Wi-Fi 模块(ESP8266)
https://github.com/Security-Onion-Solutions/security-onion 基于 ubuntu 用于入侵检测，网络安全监控和日志管理，采用分布式架构
https://github.com/jpcertcc/sysmonsearch 将 Sysmon 的日志结果可视化
http://m.imooc.com/article/21236 快速自检电脑是否被黑客入侵过(Windows 版)
http://www.freebuf.com/articles/system/157597.html 快速自检电脑是否被黑客入侵过（Linux 版）
http://www.freebuf.com/rookie/179638.html 服务器入侵溯源小技巧整理
https://github.com/zhanghaoyil/Hawk-I 基于无监督机器学习算法从 Web 日志中自动提取攻击 Payload
```

恶意文件测与样本分析

```
https://github.com/open-power-workgroup/Hospital 全国莆田系医院名单
https://github.com/chenerlich/FCL 恶意代码使用的命令行收集
https://paper.seebug.org/421 常见软件合集与恶意软件分析
https://github.com/sapphirex00/Threat-Hunting apt 恶意软件样本
https://www.malware-traffic-analysis.net/ 恶意软件样本
http://dasmalwerk.eu/ 恶意软件样本
https://github.com/ytisf/theZoo 恶意软件样本
https://github.com/mstfknn/malware-sample-library 恶意软件样本
http://99.248.235.4/Library/ 恶意软件样本库。ladder
https://github.com/robbyFux/Ragpicker 恶意软件信息爬取汇总分析
https://github.com/phage-nz/ph0neutria 恶意软件信息爬取汇总分析
https://github.com/JR0driguezB/malware_configs 常见恶意配置文件
https://github.com/sfaci/masc 扫描网站中的恶意软件，以及其他一些网站维护功能
https://github.com/Neo23x0/munin 依据文件 Hash 从各种在线恶意软件扫描服务提取信息的工具
https://github.com/1lastBr3ath/drmine 自动化检测网页是否包含挖矿脚本的工具
https://github.com/KasperskyLab/klara 卡巴斯基开源基于 Yara 的分布式恶意软件扫描系统，
https://github.com/botherder/kraken go，实现的 Yara 恶意软件扫描器
https://github.com/alexandreborges/malwoverview simple，将恶意文件进行快速分类
https://github.com/joxeankoret/pigaios 直接对比源代码与编译的二进制文件
https://github.com/viper-framework py2，二进制分析和管理框架，对恶意文件进行分析
https://github.com/netxfly/sec_check 通过信息采集（账户、连接、端口等）与 yara 扫描进行安全检测
https://github.com/nao-sec/tknk_scanner yara 引擎为基础的恶意软件识别框架
https://github.com/felixweyne/ProcessSpawnControl powershell,对恶意程序进行检测与监控
https://github.com/Aurore54F/JaSt 使用语法检测恶意/混淆的 JS 文件，https://www.blackhoodie.re/assets/archive/JaSt_blackhoodie.pdf
http://edr.sangfor.com.cn/ win，Linux 下恶意软件、webshell 检测查杀工具
http://www.clamav.net/downloads 病毒查杀软件
http://www.chkrootkit.org/ rootkit 检测工具
http://rootkit.nl/projects/rootkit_hunter.html rootkit 检测工具
```

恶意文件检测之 Webshell 查杀扫描

```
http://www.safedog.cn/ 安全狗 web 防火墙
http://d99net.net/ win，啊 D 出品 D 盾 _ 防火墙，包含 waf 与 webshel 检测功能
https://github.com/he1m4n6a/findWebshell py，webshell 检查工具，可后期添加后门指纹，很强大
https://github.com/ym2011/ScanBackdoor 一款简洁的 Webshell 扫描工具
https://github.com/erevus-cn/scan_webshell webshell 扫描工具
https://github.com/yassineaddi/BackdoorMan 可对指定目录进行 php webshell 检测
https://github.com/nbs-system/php-malware-finder 一款高效率 PHP-webshell 扫描工具
https://github.com/emposha/PHP-Shell-Detector 测试效率高达 99%的 webshell 检测工具
https://github.com/emposha/Shell-Detector Webshell 扫描工具，支持 php/perl/asp/aspx webshell 扫描
```

压力测试与 DDOS 相关

```
https://github.com/ywjt/Dshield DDOS 防护
https://github.com/NewEraCracker/LOIC/ 一个为 Windows 设计的网络压力测试工具现已支持 Mac OS—译者注
https://github.com/649/Memcrashed-DDoS-Exploit 利用 Memcached 服务器的 DDoS 攻击工具，向 Memcached 服务器发送伪造的 UDP 数据包使其向攻击目标回复大量数据包
https://github.com/jseidl/GoldenEye py，DOS 测试
https://github.com/mschwager/dhcpwn DHCP IP 资源耗尽攻击工具
https://github.com/Microsoft/Ethr GO,跨平台,TCP，UDP，HTTP，HTTPS 压力测试工具
```

匿名信息保护洋葱路由 TorBrowser

```
https://github.com/leitbogioro/Fuck_Aliyun 关闭阿里云监控服务
https://github.com/Nummer/Destroy-Windows-10-Spying DWS 关闭 windows 监控服务
https://github.com/Rizer0/Log-killer 日志清除，Windows/Linux 服务器中的所有
https://github.com/360-A-Team/EventCleaner 日志擦除工具
https://github.com/s-rah/onionscan darkweb 暗网爬虫
https://github.com/globaleaks/Tor2web darkweb 暗网代理服务器，将 onion 的服务变为普通的服务
https://github.com/milesrichardson/docker-onion-nmap 使用 nmap 扫描 Tor 网络上隐藏的”onion”服务
https://github.com/GouveaHeitor/nipe 一个使所有流量通过 Tor 网络发出的脚本
https://github.com/trimstray/multitor 启用多个 tor 通道转发流量，并设置负载均衡
```

爬虫相关

```
https://github.com/alphardex/looter 轻量型爬虫框架，类比 Scrapy
https://github.com/luyishisi/Anti-Anti-Spider 过反爬虫
https://github.com/xchaoinfo/fuck-login 模拟登录一些常见的网站
https://github.com/Maicius/InterestingCrawler 抓取 QQ 空间说说内容并进行分析
https://github.com/xjr7670/QQzone_crawler QQ 空间动态爬虫，利用 cookie 登录获取所有可访问好友空间的动态保存到本地
```

在线自服务与工具

```
https://github.com/Kickball/awesome-selfhosted awesome 系列之自服务应用
https://github.com/littlecodersh/itchat 微信个人号接口、微信机器人及命令行微信
https://github.com/sym233/core-values-encoder js,社会主义核心价值观加密，https://sym233.github.io/core-values-encod
er/
https://github.com/valentinxxx/nginxconfig.io/ 在线 nginx 配置文件生成，demo 网址 https://nginxconfig.io
https://github.com/asciimoo/searx 搭建一个自己的搜索引擎,DEMO 网址 https://searx.me/
http://sc.ftqq.com/3.version server 酱微信通知
https://osint.link Open Source Intelligence (OSINT) Tools & Resources
https://www.wolframalpha.com 根据问题直接给出答案的网站
shodan.io 互联网感知引擎
fofa.so 白帽汇 NOSEC
https://www.oshadan.com 傻蛋联网设备搜索 _ 湖南安数网络
zoomeye.org 知道创宇互联网感知引擎
https://sms.cngrok.com/receiving-sms 收码接码
https://www.pdflibr.com/ 收码接码
https://www.fakenamegenerator.com 多国身份信息模拟器
https://recruitin.net Easily use Google to search profiles on LinkedIn
https://www.truthfinder.com 美国公民信息查询
https://verify-email.org 邮件真实性验证
https://safeweb.norton.com 诺顿网站安全检测
http://www.vuln.cn/tools/ftp 在线 FTP 登录
http://www.link114.cn/title/ 批量查询网站标题
https://www.whatweb.net/ 在线 web 指纹识别
https://hackertarget.com/ip-tools/ 提供 api，ip 相关工具、在线扫描器
http://www.webscan.cc/ 同 IP 网站查询,C 段查询,IP 反查域名,C 段旁注,旁注工具
https://www.phpinfo.me/bing.php 在线旁站查询|C 段查询|必应接口 C 段查询
https://www.phpinfo.me/domain/ 在线子域名爆破
https://www.dnsdb.io DNS 查询,子域名查询,IP 查询,A 记录查询,域名解析,旁站查询
https://dnsdumpster.com/ dns recon and research, find and lookup dns records
http://ip.chaxun.la/ ip 反查域名–查询啦
https://habo.qq.com 在线恶意文件检测
https://www.virustotal.com 恶意软件检测
http://r.virscan.org/ 恶意软件检测
https://www.appscan.io 移动软件在线检测
https://www.nomoreransom.org 常见勒索软件分析还原
https://www.cmd5.com/ HASH 密码在线破解
https://www.onlinehashcrack.com 密码哈希在线破解，邮件通知
```

在线办公套件

```
https://sadd.io/ 在线操作系统
https://github.com/zyx0814/dzzoffice 在线办公套件,DEMO 网址 demo.dzzoffice.com
https://github.com/RobbieHan/gistandard py，基于 Django，OA 工单办公管理系统
https://github.com/pavanw3b/sh00t PY3,DJANGO，安全测试工单管理
https://github.com/chaitin/strapdown-zeta 基于 strapdown.js，长亭二次开发开源的 Wiki 系统，支持 markdown
https://etherpad.net/ 在线可编辑记事本
https://www.upload.ee/ 文件共享平台
https://github.com/micahflee/onionshare 利用 onion 洋葱服务器匿名文件共享
https://github.com/filebrowser/filebrowser GO,基于 Caddy 框架的网盘
https://github.com/nextcloud/server php，私有云网盘，owncloud 分支
https://github.com/owncloud/core php，私有云网盘，界面不美观
https://github.com/haiwen/seafile C,私有云网盘，速度快，功能少
https://github.com/ymfe/yapi API 管理工具
https://thyrsi.com/ 图片上传分享工具
```

隐私匿名加密

```
https://www.lshack.cn/118/ 在线接收验证码/邮箱/粘贴板/文件传输大集合。
http://bccto.me 一次性邮箱
https://www.guerrillamail.com 一次性邮箱
http://24mail.chacuo.net/ 一次性邮箱
http://www.yopmail.com 一次性邮箱
https://yandex.com/ 非手机邮箱
https://mail.ru/ 非手机邮箱
https://mail.protonmail.com/login 非手机邮箱
https://github.com/walkor/workerman-chat php，在线聊天室，可扩展
https://github.com/hack-chat https://hack.chat/?your-channel js,在线聊天，问号后面跟你的房间名
https://github.com/akaxincom/openzaly java,聊天室，Akaxin 为客户端闭源
https://github.com/RocketChat/Rocket.Chat js,在线团队聊天服务器，https://rocket.chat/install
https://telegram.org
https://www.whatsapp.com
https://wire.com/en
https://signal.org
http://www.batmessenger.com
http://sid.co
```

在线资源

```
https://github.com/DoubleLabyrinth/navicat-keygen navicat 注册机
https://github.com/DoubleLabyrinth/MobaXterm-keygen MobaXterm 注册机
http://www.zdfans.com zd423 - 软件分享平台领跑者
https://www.flaticon.com 免费图标网站
https://msdn.itellyou.cn 原生镜像
https://www.freenom.com 注册免费域名，dns 解析
https://codebeautify.org 在线代码美化
http://patorjk.com Text to ASCII Art Generator
https://www.seopojie.com SPAM,SEO
```

关于我

欢迎关注公众号