攻击资源合集

原创

白术macro 于 2019-02-28 20:32:00 发布 2686 收藏 14

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://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/Icamry/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

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

image.gif

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

image

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

image

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

image

image.gif

image.gif

image.gif

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

image

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

image

image.gif

image.gif

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

image

网站克隆镜像伪造

- http://www.httrack.com 网站克隆镜像

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

image

image.gif

image.gif

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 Trans 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

image

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

image

image.gif

image.gif

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

image

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

image

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

image

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

image

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

image

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

image

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

image

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

image

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

image