常用工具匯總

手機黑客 昨天

> **來文章源：安全初心**

目錄

漏洞及滲透平台

WebGoat漏洞練習環境

https://github.com/WebGoat/WebGoat

https://github.com/WebGoat/WebGoat-Legacy

該死的易受攻擊的Web應用程序(漏洞練習平台)

https://github.com/RandomStorm/DVWA

數據庫注入練習平台

https://github.com/Audi-1/sqli-labs

用node寫的漏洞練習平台，類似OWASP Node Goat

https://github.com/cr0hn/vulnerable-node

花式掃描器

端口掃描器Nmap

https://github.com/nmap/nmap

本地網絡掃描器

https://github.com/SkyLined/LocalNetworkScanner

子域名掃描器

https://github.com/lijiejie/subDomainsBrute

漏洞輸入掃描器

https://github.com/jh00nbr/Routerhunter-2.0

演示信息屏幕截圖

https://github.com/lijiejie/BBScan

Waf類型檢測工具

https://github.com/EnableSecurity/wafw00f

信息搜集工具

社工插件，可查找以email、phone、username的注册的所有网站账号信息

https://github.com/n0tr00t/Sreg

Github信息搜集，可实时扫描查询git最新上传有关邮箱账号密码信息

https://github.com/sea-god/gitscan

github Repo信息搜集工具

https://github.com/metac0rtex/GitHarvester

WEB工具

webshell大合集

https://github.com/tennc/webshell

渗透以及web攻击脚本

https://github.com/brianwrf/hackUtils

web渗透小工具大合集

https://github.com/rootphantomer/hack*tools*for_me

XSS数据接收平台

https://github.com/firesunCN/BlueLotus_XSSReceiver

XSS与CSRF工具

https://github.com/evilcos/xssor

Short for command injection exploiter，web向命令注入检测工具

https://github.com/stasinopoulos/commix

数据库注入工具

https://github.com/sqlmapproject/sqlmap

Web代理，通过加载sqlmap api进行sqli实时检测

https://github.com/zt2/sqli-hunter

新版中国菜刀

https://github.com/Chora10/Cknife

.git泄露利用EXP

https://github.com/lijiejie/GitHack

浏览器攻击框架

https://github.com/beefproject/beef

自动化绕过WAF脚本

https://github.com/khalilbijjou/WAFNinja

http命令行客户端，可以从命令行构造发送各种http请求（类似于Curl）

https://github.com/jkbrzt/httpie

浏览器调试利器

https://github.com/firebug/firebug

一款开源WAF

https://github.com/SpiderLabs/ModSecurity

windows域渗透工具

windows渗透神器

https://github.com/gentilkiwi/mimikatz

Powershell渗透库合集

https://github.com/PowerShellMafia/PowerSploit

Powershell tools合集

https://github.com/clymb3r/PowerShell

Fuzz

Web向Fuzz工具

https://github.com/xmendez/wfuzz

HTTP暴力破解，撞库攻击脚本

https://github.com/lijiejie/htpwdScan

漏洞利用及攻击框架

msf

https://github.com/rapid7/metasploit-framework

Poc调用框架，可加载Pocsuite,Tangscan，Beebeeto等

https://github.com/erevus-cn/pocscan

Pocsuite

https://github.com/knownsec/Pocsuite

Beebeeto

https://github.com/n0tr00t/Beebeeto-framework

漏洞POC&EXP

ExploitDB官方git版本

https://github.com/offensive-security/exploit-database

php漏洞代码分析

https://github.com/80vul/phpcodz

Simple test for CVE-2016-2107

https://github.com/FiloSottile/CVE-2016-2107

CVE-2015-7547 POC

https://github.com/fjserna/CVE-2015-7547

JAVA反序列化POC生成工具

https://github.com/frohoff/ysoserial

JAVA反序列化EXP

https://github.com/foxglovesec/JavaUnserializeExploits

Jenkins CommonCollections EXP

https://github.com/CaledoniaProject/jenkins-cli-exploit

CVE-2015-2426 EXP (windows内核提权)

https://github.com/vlad902/hacking-team-windows-kernel-lpe

use docker to show web attack(php本地文件包含结合phpinfo getshell 以及ssrf结合curl的利用演示)

https://github.com/hxer/vulnapp

php7缓存覆写漏洞Demo及相关工具

https://github.com/GoSecure/php7-opcache-override

XcodeGhost木马样本

https://github.com/XcodeGhostSource/XcodeGhost

中间人攻击及钓鱼

中间人攻击框架

https://github.com/secretsquirrel/the-backdoor-factory

https://github.com/secretsquirrel/BDFProxy

https://github.com/byt3bl33d3r/MITMf

Inject code, jam wifi, and spy on wifi users https://github.com/DanMcInerney/LANs.py

可扩展的中间人代理工具

https://github.com/intrepidusgroup/mallory

wifi钓鱼

https://github.com/sophron/wifiphisher

密码破解

密码破解工具

https://github.com/shinnok/johnny

本地存储的各类密码提取利器

https://github.com/AlessandroZ/LaZagne

二进制及代码分析工具

二进制分析工具

https://github.com/devttys0/binwalk

系统扫描器，用于寻找程序和库然后收集他们的依赖关系，链接等信息

https://github.com/quarkslab/binmap

rp++ is a full-cpp written tool that aims to find ROP sequences in PE/Elf/Mach-O (doesn't support the FAT binaries) x86/x64 binaries.

https://github.com/0vercl0k/rp

Windows Exploit Development工具

https://github.com/lillypad/badger

二进制静态分析工具（python）

https://github.com/bdcht/amoco

Python Exploit Development Assistance for GDB

https://github.com/longld/peda

对BillGates Linux Botnet系木马活动的监控工具

https://github.com/ValdikSS/billgates-botnet-tracker

木马配置参数提取工具

https://github.com/kevthehermit/RATDecoders

Shellphish编写的二进制分析工具（CTF向）

https://github.com/angr/angr

针对python的静态代码分析工具

https://github.com/yinwang0/pysonar2

一个自动化的脚本（shell）分析工具，用来给出警告和建议

https://github.com/koalaman/shellcheck

基于AST变换的简易Javascript反混淆辅助工具

https://github.com/ChiChou/etacsufbo

EXP编写框架及工具

二进制EXP编写工具

https://github.com/t00sh/rop-tool

CTF Pwn 类题目脚本编写框架

https://github.com/Gallopsled/pwntools

an easy-to-use io library for pwning development

https://github.com/zTrix/zio

跨平台注入工具（ Inject JavaScript to explore native apps on Windows, Mac, Linux, iOS and Android.）

https://github.com/frida/frida

隐写相关工具

隐写检测工具

https://github.com/abeluck/stegdetect

各类安全资料

域渗透教程

https://github.com/l3m0n/pentest_study

python security教程（原文链接http://www.primalsecurity.net/tutorials/python-tutorials/）

https://github.com/smartFlash/pySecurity

data_hacking合集

https://github.com/ClickSecurity/data_hacking

mobile-security-wiki

https://github.com/exploitprotocol/mobile-security-wiki

书籍《reverse-engineering-for-beginners》

https://github.com/veficos/reverse-engineering-for-beginners

一些信息安全标准及设备配置

https://github.com/luyg24/IT_security

APT相关笔记

https://github.com/kbandla/APTnotes

Kcon资料

https://github.com/knownsec/KCon

ctf及黑客资源合集

https://github.com/bt3gl/My-Gray-Hacker-Resources

ctf和安全工具大合集

https://github.com/zardus/ctf-tools

《DO NOT FUCK WITH A HACKER》

https://github.com/citypw/DNFWAH

各类CTF资源

近年ctf writeup大全

https://github.com/ctfs/write-ups-2016

https://github.com/ctfs/write-ups-2015

https://github.com/ctfs/write-ups-2014

fbctf竞赛平台Demo

https://github.com/facebook/fbctf

ctf Resources

https://github.com/ctfs/resources

各类编程资源

大礼包（什么都有）

https://github.com/bayandin/awesome-awesomeness

bash-handbook

https://github.com/denysdovhan/bash-handbook

python资源大全

https://github.com/jobbole/awesome-python-cn

git学习资料

https://github.com/xirong/my-git

安卓开源代码解析

https://github.com/android-cn/android-open-project-analysis

python框架，库，资源大合集

https://github.com/vinta/awesome-python

JS 正则表达式库（用于简化构造复杂的JS正则表达式）

https://github.com/VerbalExpressions/JSVerbalExpressions

Python

python 正则表达式库（用于简化构造复杂的python正则表达式）

https://github.com/VerbalExpressions/PythonVerbalExpressions

python任务管理以及命令执行库

https://github.com/pyinvoke/invoke

python exe打包库

https://github.com/pyinstaller/pyinstaller

py3 爬虫框架

https://github.com/orf/cyborg

一个提供底层接口数据包编程和网络协议支持的python库

https://github.com/CoreSecurity/impacket

python requests 库

https://github.com/kennethreitz/requests

python 实用工具合集

https://github.com/mahmoud/boltons

python爬虫系统

https://github.com/binux/pyspider

ctf向 python工具包

https://github.com/P1kachu/v0lt

科学上网

科学上网工具

https://github.com/XX-net/XX-Net

老司机福利

微信自动抢红包动态库

https://github.com/east520/AutoGetRedEnv

微信抢红包插件（安卓版）

https://github.com/geeeeeeeeek/WeChatLuckyMoney

神器

https://github.com/yangyangwithgnu/hardseed

其他

以下内容来自：https://github.com/We5ter/Scanners-Box/blob/master/README_CN.md 子域名枚举类

https://github.com/lijiejie/subDomainsBrute (经典的子域名爆破枚举脚本)

https://github.com/ring04h/wydomain (子域名字典穷举)

https://github.com/le4f/dnsmaper (子域名枚举与地图标记)

https://github.com/0xbug/orangescan (在线子域名信息收集工具)

https://github.com/TheRook/subbrute （根据DNS记录查询子域名)

https://github.com/We5ter/GoogleSSLdomainFinder (基于谷歌SSL透明证书的子域名查询脚本)

https://github.com/mandatoryprogrammer/cloudflare_enum （使用CloudFlare进行子域名枚举的脚本）

https://github.com/18F/domain-scan (A domain scanner)

https://github.com/Evi1CLAY/Cool ... Python/DomainSeeker（多方式收集目标子域名信息）

数据库漏洞扫描类

https://github.com/0xbug/SQLiScanner (一款基于SQLMAP和Charles的被动SQL注入漏洞扫描工具)

https://github.com/stamparm/DSSS (99行代码实现的sql注入漏洞扫描器)

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（攻击SQLSERVER的Powershell脚本框架）

弱口令或信息泄漏扫描类

https://github.com/lijiejie/htpwdScan (一个简单的HTTP暴力破解、撞库攻击脚本)

https://github.com/lijiejie/BBScan (一个迷你的信息泄漏批量扫描脚本)

https://github.com/lijiejie/GitHack (.git文件夹泄漏利用工具)

https://github.com/wilson9x1/fenghuangscanner_v3 (端口及弱口令检测)

https://github.com/ysrc/F-Scrack (对各类服务进行弱口令检测的脚本)

https://github.com/Mebus/cupp （根据用户习惯生成弱口令探测字典脚本）

https://github.com/RicterZ/genpAss （中国特色的弱口令生成器）

https://github.com/netxfly/crack_ssh （go写的协程版的ssh\redis\mongodb弱口令破解工具）

物联网设备扫描

https://github.com/rapid7/IoTSeeker （物联网设备默认密码扫描检测工具)

https://github.com/shodan-labs/iotdb (使用nmap扫描IoT设备）

xss扫描器

https://github.com/shawarkhanethicalhacker/BruteXSS （Cross-Site Scripting Bruteforcer） https://github.com/1N3/XSSTracer (A small python script to check for Cross-Site Tracing)

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）

企业网络自检

https://github.com/sowish/LNScan （详细的内部网络信息扫描器）

https://github.com/ysrc/xunfeng (网络资产识别引擎，漏洞检测引擎）

https://github.com/SkyLined/LocalNetworkScanner (javascript实现的本地网络扫描器)

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/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）

webshell检测

https://github.com/We5ter/Scanners-Box/tree/master/Find_webshell/ （php后门检测，脚本较简单，因此存在误报高和效率低下的问题）

https://github.com/yassineaddi/BackdoorMan （A toolkit find malicious, hidden and suspicious PHP scripts and shells in a chosen destination）

内网渗透

https://github.com/0xwindows/VulScritp （企业内网渗透脚本，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/fdiskyou/hunter（调用 Windows API 枚举用户登录信息）

中间件扫描、指纹识别类

https://github.com/ring04h/wyportmap (目标端口扫描+系统服务指纹识别)

https://github.com/ring04h/weakfilescan (动态多线程敏感信息泄露检测工具)

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/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/OffensivePython/Nscan (a fast Network scanner inspired by Masscan and Zmap)

https://github.com/ywolf/F-NAScan (网络资产信息扫描, ICMP存活探测,端口扫描，端口指纹服务识别）

https://github.com/ywolf/F-MiddlewareScan （中间件扫描）

https://github.com/maurosoria/dirsearch (Web path scanner)

https://github.com/x0day/bannerscan （C段Banner与路径扫描）

https://github.com/RASSec/RASscan (端口服务扫描)

https://github.com/3xp10it/bypass_waf （waf自动暴破）

https://github.com/3xp10it/mytools/blob/master/xcdn.py（获取cdn背后的真实ip）

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/Xyntax/DirBrute（多线程WEB目录爆破工具）

https://github.com/zer0h/httpscan（一个爬虫式的网段Web主机发现小工具）

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）

专用扫描器

https://github.com/blackye/Jenkins (Jenkins漏洞探测、用户抓取爆破)

https://github.com/code-scan/dzscan (discuz扫描)

https://github.com/chuhades/CMS-Exploit-Framework (CMS攻击框架)

https://github.com/lijiejie/IIS*shortname*Scanner (an IIS shortname Scanner)

https://github.com/We5ter/Scanne ... ter/FlashScanner.pl (flashxss扫描)

https://github.com/coffeehb/SSTIF（一个Fuzzing服务器端模板注入漏洞的半自动化工具）

无线网络

https://github.com/savio-code/fern-wifi-cracker/ (无线安全审计工具)

https://github.com/m4n3dw0lf/PytheM（Python网络/渗透测试工具）

https://github.com/P0cL4bs/WiFi-Pumpkin（无线安全渗透测试套件）

综合类

https://github.com/az0ne/AZScanner (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/blackye/lalascan (自主开发的分布式web漏洞扫描框架，集合owasp top10漏洞扫描和边界资产发现能力)

https://github.com/blackye/BkScanner (BkScanner 分布式、插件化web漏洞扫描器)

https://github.com/ysrc/GourdScanV2 （被动式漏洞扫描)

https://github.com/alpha1e0/pentestdb (WEB渗透测试数据库)

https://github.com/netxfly/passive_scan (基于http代理的web漏洞扫描器)

https://github.com/1N3/Sn1per (自动化扫描器，包括中间件扫描以及设备指纹识别)

https://github.com/RASSec/pentestEr_Fully-automatic-scanner（定向全自動化滲透測試工具）

https://github.com/3xp10it/3xp10it （3xp10it自動化滲透測試框架）

https://github.com/Lcys/lcyscan（python插件化漏洞掃描器）

https://github.com/Xyntax/POC-T（滲透測試插件化框架）

周大福平台 http://www.shiyanbar.com/

http://oj.xctf.org.cn/

http://ctf.bugku.com/

http://rookiehacker.org/

如侵權請私聊公眾號

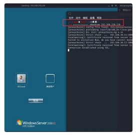
喜歡這個內容的人還喜歡

十年黑大佬的網絡安全滲透技術分享

Linux網絡安全

一次簡單的內網靶場實戰

瀟湘信安



自動化掃描工具 -Sn1per

移動雲筆記