通用工具

工具类型	工具地址	更新时间
内网扫描	https://github.com/shadow1ng/fscan	2022-07-06
哥斯拉Webshell管理	https://github.com/BeichenDream/Godzilla	2021-11-01
ARL 资产侦察灯塔	https://github.com/TophantTechnology/ARL	2022-08-25
aliyun-accesskey-Tools	https://github.com/mrknow001/aliyun-accesskey-Tools	2021-09-28
PEASS-ng 提权套装	https://github.com/carlospolop/PEASS-ng	2022-09-11
nuclei 漏洞扫描器	https://github.com/projectdiscovery/nuclei	2022-08-26
railgun 渗透集成化工具	https://github.com/lz520520/railgun	2022-08-22
YAKIT 网络安全单兵工具	https://github.com/yaklang/yakit	2022-09-16
EHole（棱洞）3.0 指纹探测工具	https://github.com/EdgeSecurityTeam/EHole	2021-06-23
Traitor 提权工具	https://github.com/liamg/traitor	2022-03-09
Stowaway 内网穿透	https://github.com/ph4ntonn/Stowaway	2022-04-08
CF 云环境利用框架	https://github.com/teamssix/cf	2022-09-07
Naabu 端口扫描	https://github.com/projectdiscovery/naabu	2022-07-31
httpx HTTP状态获取	https://github.com/projectdiscovery/httpx	2022-08-01
Malleable C2 Profiles	https://github.com/xx0hcd/Malleable-C2-Profiles	2022-09-10
shuize（水泽） 信息收集	https://github.com/0x727/ShuiZe_0x727	2021-08-03

工具类型	工具地址	更新时间
Cloud-Bucket-Leak-Detection-Tools	https://github.com/UzJu/Cloud-Bucket-Leak-Detection-Tools	2022-07-16
SharpHostInfo 内网主机探测	https://github.com/shmilylty/SharpHostInfo	2022-09-09
pocsuite3	https://github.com/knownsec/pocsuite3	2022-09-08
URLFinder	https://github.com/pingc0y/URLFinder	2022-09-16
ALLiN 扫描工具	https://github.com/P1-Team/AlliN	2022-07-26
ihoneyBakFileScan 备份文件泄露扫描	https://github.com/VMsec/ihoneyBakFileScan_Modify	2022-09-15
spark（火花） 自动字典生成器	https://github.com/G0mini/spark	2022-09-13
Exphub 漏洞利用脚本	https://github.com/zhzyker/exphub	2021-04-04
EasyPen 综合利用工具	https://github.com/lijiejie/EasyPen	2022-09-16
Dog Tunnel(狗洞)端口映射工具	https://github.com/vzex/dog-tunnel	2020-05-22
frp 端口映射工具	https://github.com/fatedier/frp	2022-07-11
MYExploit 综合利用工具	https://github.com/achuna33/MYExploit	2022-09-20
dirsearch 目录扫描工具	https://github.com/maurosoria/dirsearch	2022-10-05
OneForAll 子域收集工具	https://github.com/shmilylty/OneForAll	2022-07-10
Cloud-Bucket-Leak-Detection-Tools 云储存利用工具	https://github.com/UzJu/Cloud-Bucket-Leak-Detection-Tools	2022-07-16
ObserverWard 指纹识别工具	https://github.com/0x727/ObserverWard	2022-09-27
AtlasC2 C2框架Atlas	https://github.com/Gr1mmie/AtlasC2	2022-04-05
Goblin 钓鱼演练工具	https://github.com/xiecat/goblin	2022-07-13

工具类型	工具地址	更新时间
AsamF 资产收集工具	https://github.com/Kento-Sec/AsamF	2022-09-22
Httpx IP、Url批量存活探测	https://github.com/projectdiscovery/httpx	2022-08-01
Ghidra 软件逆向工程框架	https://github.com/NationalSecurityAgency/ghidra	2022-07-27
crack 弱口令爆破工具	https://github.com/niudaii/crack	2022-09-06
Empire 后开发框架	https://github.com/BC-SECURITY/Empire	2022-08-31
ksubdomain 子域名爆破工具	https://github.com/knownsec/ksubdomain	2021-01-12
scan4all 综合扫描	https://github.com/hktalent/scan4all	2022-10-15
Kscan 资产测绘工具	https://github.com/lcvvvv/kscan	2022-05-19
RedGuard C2流量前置工具	https://github.com/wikiZ/RedGuard	2022-08-04
VScan 漏洞扫描工具	https://github.com/veo/vscan	2022-06-23
pydictor 字典建立工具	https://github.com/LandGrey/pydictor	2017-12-20
AutoPWN Suite 漏扫利用工具	https://github.com/GamehunterKaan/AutoPWN-Suite	2022-09-09
CloudFlair 找CF真实IP工具	https://github.com/christophetd/CloudFlair	2021-12-08
feroxbuster 目录扫描工具	https://github.com/epi052/feroxbuster	2022-05-22
POC-bomber 漏洞检测/利用工具	https://github.com/tr0uble-mAker/POC-bomber	2022-09-13
iox 端口转发工具	https://github.com/EddieIvan01/iox	2020-09-22
f8x 一键环境搭建	https://github.com/ffffffff0x/f8x	2020-09-04
URL 搜集工具	https://github.com/lc/gau	2022-07-24

工具类型	工具地址	更新时间
子域名发现工具	https://github.com/projectdiscovery/subfinder	2022-10-17
pocassist POC框架	https://github.com/jweny/pocassist	2021-08-11
Gobuster 目录文件、DNS和VHost爆破工具	https://github.com/OJ/gobuster	2022-10-29
Vulmap web漏洞扫描和验证工具	https://github.com/zhzyker/vulmap	2021-09-01
ESP32 Wi-Fi攻击工具	https://github.com/risinek/esp32-wifi-penetration-tool	2021-05-05
牛屎花 C2远控	https://github.com/YDHCUI/manjusaka	2022-10-10
Amass 资产发现、子域名扫描工具	https://github.com/OWASP/Amass	2022-09-23
GitHack Git泄露利用工具	https://github.com/lijiejie/GitHack	2022-05-09
subDomainsBrute 子域名爆破工具	https://github.com/lijiejie/subDomainsBrute	2022-06-05
JNDI-Inject-Exploit 反序列化测试工具	https://github.com/exp1orer/JNDI-Inject-Exploit	2021-12-29
LadonGo 内网渗透扫描器框架	https://github.com/k8gege/LadonGo	2022-07-28
Dismap 资产发现及指纹识别	https://github.com/zhzyker/dismap	2022-06-16
afrog 漏洞扫描工具	https://github.com/zan8in/afrog	2022-10-18
TruffleHog 敏感信息搜集工具	https://github.com/trufflesecurity/trufflehog	2022-11-09
Komo 综合资产收集和漏洞扫描工具	https://github.com/komomon/Komo	2022-10-24
xray 被动扫描安全评估工具	https://github.com/chaitin/xray	2022-10-14
AppInfoScanner 移动端信息收集扫描工具	https://github.com/kelvinBen/AppInfoScanner	2022-10-23
Linux提权exp	https://github.com/Al1ex/LinuxEelvation	2022-07-29

工具类型	工具地址	更新时间
Packer Fuzzer Webpack网站扫描工具	https://github.com/rtcatc/Packer-Fuzzer	2022-06-19
Polaris 信息搜集与漏洞利用框架	https://github.com/doimet/Polaris	2022-10-07
geacon_pro 免杀工具	https://github.com/H4de5-7/geacon_pro	2022-11-10
spp 隧道代理工具	https://github.com/esrrhs/spp	2021-09-28
Payer 子域名挖掘机	https://github.com/Pik-sec/Payer	2022-10-15
MobSF 移动安全测试框架	https://github.com/MobSF/Mobile-Security-Framework-MobSF	2022-10-04
ByPassGodzilla/哥斯拉免杀生成	https://github.com/Tas9er/ByPassGodzilla	2022-11-01
katana 下一代爬虫框架	https://github.com/projectdiscovery/katana	2023-01-13
SourceDetector 自动发现.map文件	https://github.com/SunHuawei/SourceDetector	2021-07-02
windows提权漏洞检测	https://github.com/bitsadmin/wesng	2023-01-11
API未授权扫描插件	https://github.com/API-Security/APIKit	2023-01-16
Dirmap web目录扫描工具	https://github.com/H4ckForJob/dirmap	2022-06-01
vshell c2主机群管理工具	https://github.com/veo/vshell	2022-12-24
Yasso 内网渗透辅助工具集	https://github.com/sairson/Yasso	2022-06-29
JSFinder 信息收集接口	https://github.com/Threezh1/JSFinder	2022-12-11
Perun 综合扫描器	https://github.com/WyAtu/Perun	2019-04-25
AntSword 加载器	https://github.com/AntSwordProject/antSword-Loader	2019-04-24
AntSword	https://github.com/AntSwordProject/antSword	2022-07-17

工具类型	工具地址	更新时间
Goby 漏洞扫描	https://github.com/gobysec/Goby	2023-01-17
goby exp库	https://github.com/k3vi-07/goby-exp	2021-08-26
reNgine 自动侦察框架	https://github.com/yogeshojha/rengine	2022-12-30
SatanSword 红队综合渗透框架	https://github.com/Lucifer1993/SatanSword	2022-04-02
Dirscan 目录扫描	https://github.com/corunb/Dirscan	2022-11-14
LSTAR CobaltStrike综合后渗透插件	https://github.com/lintstar/LSTAR	2022-06-15
Platypus 交互式反向 Shell 管理器	https://github.com/WangYihang/Platypus	2021-07-17
Phoenix 新一代目录扫描神器	https://github.com/Pik-sec/Phoenix	2022-10-15
RouteVulScan 递归式被动检测脆弱路径的bp插件	https://github.com/F6JO/RouteVulScan	2023-01-08
MDUT 数据库跨平台利用工具	https://github.com/SafeGroceryStore/MDUT	2022-06-22
LaZagne 密码凭证收集工具	https://github.com/AlessandroZ/LaZagne	2019-09-16
Erfrp frp二开-免杀与隐藏	https://github.com/Goqi/Erfrp	2022-11-18
EventCleaner 日志清理	https://github.com/QAX-A-Team/EventCleaner	2018-09-07
UACMe Windows bypassUAC	https://github.com/hfiref0x/UACME	2022-07-17
SCAMagicScan POC漏洞扫描工具	https://github.com/SCAMagic/SCAMagicScan	2023-01-18
ENScan Go 企业信息搜集工具	https://github.com/wgpsec/ENScan_GO	2022-12-02
ThunderSearch 闪电搜索器	https://github.com/xzajyjs/ThunderSearch	2022-11-08
EmailAll 邮箱收集工具	https://github.com/Taonn/EmailAll	2022-02-24

工具类型	工具地址	更新时间
finger 资产识别工具	https://github.com/EASY233/Finger	2022-09-19
apk扫描器	https://github.com/dwisiswant0/apkleaks	2021-08-11
Neo-reGeorg 代理工具	https://github.com/L-codes/Neo-reGeorg	2022-12-25
blasting 图形化后台爆破工具	https://github.com/gubeihc/blasting	2023-01-02
HaE 敏感信息收集 burp插件	https://github.com/gh0stkey/HaE	2022-12-18
powershell免杀混淆	https://github.com/H4de5-7/powershell-obfuscation	2023-01-17
Bundler-bypass 免杀捆绑器	https://github.com/H4de5-7/Bundler-bypass	2022-11-08
java图形化漏洞利用工具集	https://github.com/savior-only/javafx_tools	2022-08-05

漏洞利用

漏洞产品	工具地址	更新时间
SpringBootExploit	https://github.com/0x727/SpringBootExploit	2022-04-17
Springboot漏洞全家桶	https://github.com/woodpecker-appstore/springboot-vuldb	2021-05-24
Log4j2Scan	https://github.com/whwlsfb/Log4j2Scan	2022-09-02
ShiroExploit	https://github.com/feihong-cs/ShiroExploit-Deprecated	2020-10-04
ShiroAttack2	https://github.com/SummerSec/ShiroAttack2	2022-08-31
thinkphp_gui_tools	https://github.com/bewhale/thinkphp_gui_tools	2022-08-18
Fastjson-Patrol	https://github.com/ce-automne/FastjsonPatrol	2022-04-01

漏洞产品	工具地址	更新时间
Vmware虚拟化漏洞利用（HCX/vCenter/NSX/Horizon/vRealize）	https://github.com/NS-Sp4ce/Vm4J	2022-01-07
Struts2-Scan 漏洞检测	https://github.com/HatBoy/Struts2-Scan	2020-12-23
Fastjson 扫描器	https://github.com/a1phaboy/FastjsonScan	2022-09-20
致远OA综合利用工具	https://github.com/Summer177/seeyon_exp	2021-01-03
泛微OA综合利用脚本	https://github.com/z1un/weaver_exp	2021-06-29