

hack-er-tools - some tools for emergency response

USE AT YOUR OWN RISK!

工具/资源皆来源于网络

部分工具较大，只提供下载链接

欢迎大家补充和推荐！

- [AV\(av/\)](#)
- [信息收集\(getinfo/\)](#)
- [日志分析\(log-check/\)](#)
- [进程分析\(process-check/\)](#)
- [webshell检测\(webshell-check/\)](#)
- [挖矿检测\(miner-check/\)](#)
- [勒索检测\(ransomware-check/\)](#)
- [RAT检测\(rat-check/\)](#)
- [EXP检测\(exp-check/\)](#)
- [综合分析工具\(synthesis/\)](#)
- [misc\(misc/\)](#)
- [病毒分析](#)
- [威胁情报](#)
- [勒索解密](#)
- [病毒样本](#)
- [动态](#)
- [相关项目](#)

AV(av/)

clamav.tar.gz : linux下的杀毒软件

hrsword.exe : 火绒剑

md_setup_en.exe : 360的，类似火绒剑，只能32位win使用

safedogwzApache.exe : 安全狗apache版

SfabAntiBot_x64(x86).7z : 深信服的查杀软件

卡巴斯基 : <http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe>

大蜘蛛 : <http://free.drweb.ru/download+cureit+free>

火绒安全软件 : <https://www.huorong.cn>

360杀毒 : http://sd.360.cn/download_center.html

asiainfo-sec : <http://support.asiainfo-sec.com/Anti-Virus/>

信息收集(getinfo/)

Emergency-master : 应急响应信息收集的脚本

GScan-master : 实现主机侧Checklist的自动全面化检测

LinEnum-master : Scripted Local Linux Enumeration & Privilege Escalation Checks

LinuxCheck-master : 一个linux信息搜集小脚本 主要用于应急响应

日志分析(log-check/)

Fastir_Collector_Linux-master : This tool collects different artefacts on live Linux and records the results in csv files

logC

LogViewer : 一个通用的日志查看器

LPSV2.D2

OkCat : 强大的日志处理组件

misc : 收集的一些杂项日志分析工具

Request-log-analyzer : This is a simple command line tool to analyze request log files in various formats to produce a performance report

SR_LogAnalyzer : 辅助网络安全应急响应，自动化的分析日志，找出入侵行为

USBLogView v1.25 : USBLogView is a small utility that runs in the background and records the details of any USB device that is plugged or unplugged into your system

web/apache : 一些apache日志分析工具

web/iis : 一些iis日志分析工具

web/nginx : 一些nginx日志分析工具

web/tomcat : 一些tomcat日志分析工具

AWStats : AWStats (Advanced Web Statistics) is a powerful, full-featured web server logfile analyzer which shows you all your Web statistics

GoAccess : real-time web log analyzer

web-log-parser : 开源的分析web日志工具，采用python语言开发，具有灵活的日志格式配置

windows/ : 一些windows系统日志分析工具

linux/ : 一些linux系统日志分析工具

xingtu_full

xlog : 基于flex & bison的web日志扫描工具

进程分析(process-check/)

Process Hacker : a powerful free and open source process viewer

processlassosetup64.exe

流量检测

wireshark

rootkit检测(rat-check/)

chkrootkit-m 0.2 : a chkrootkit Python port for mobile phones

rkhunter-1.4.6.tar.gz

Tyton : Linux Kernel-Mode Rootkit Hunter for 4.4.0-31+

webshell检测(webshell-check/)

d-dun/ : d盾

hm/ : 河马webshell扫描器

PHP-Shell-Detector-master.zip : Web Shell Detector

safedog/ : 安全狗

WebShellKillerForLinux.tar.gz

WebShellKillerTool.rar

sangfor : http://edr.sangfor.com.cn/backdoor_detection.html

Safe3

挖矿检测(miner-check/)

DDG_MalWare_Clean_Tool-master.zip

whatMiner-master.zip : 整理和收集遇见的各种恶意挖矿样本以供研究和学习之用

勒索检测(ransomware-check/)

banlangen : 一个基于注册表, 用于免疫WannaCrypt勒索蠕虫的小脚本

BDGandCrabDecryptTool.exe

clear_seasame.sh

RAT检测(rat-check/)

rat-check/

EXP检测(exp-check/)

linux-exploit-suggester-master.zip

Windows-Exploit-Suggester-master.zip

wesng-master.zip : Windows Exploit Suggester - Next Generation (WES-NG)

综合分析工具(synthesis/)

EmergencyResponse-master.zip

LinuxEmergency : Linux下的应急工具, 支持CentOS系统和RedHat系统

linux : linux安全检查

Loki : Simple IOC Scanner

Lynis : Security auditing and hardening tool, for UNIX-based systems.

PCHunter_free.zip

PowerTool_2.0_PortableSoft.7z

security_check : 收集各类安全检查脚本

SysinternalsSuite.zip : microsoft的工具包

VirusCheckTools : 基于行为特征进行快速匹配病毒专杀工具

windows-emergency-servicetools-master.zip : windows下一款可视化, 一键检测辅助应急工具, 生成数据采集、关联报告

Windowsxtaqjcb_bat_jb51.rar : windows系统安全检查

yingji

yingji-master.zip

应急工具集

misc(misc/)

autorun : 启动项分析

danderspritz-evtx : Parse evtx files and detect use of the DanderSpritz `eventloggedit` module

dfirtriage : Digital forensic acquisition tool for Windows-based incident response.

LogonTracer : Investigate malicious logon by visualizing and analyzing Windows active directory event logs.

radare2-master.zip : r2 is a rewrite from scratch of radare in order to provide a set of libraries and tools to work with binary files

SafetyDump : SafetyDump is an in-memory process memory dumper

skpd : Process dump to executable ELF for linux

Volatility : Volatile memory extraction utility framework

autopsy : kali自带的取证工具 <https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.14.0/autopsy-4.14.0.zip>

病毒分析

<https://www.virustotal.com/zh-cn/>

<http://www.virscan.org/language/zh-cn/about>

<https://habo.qq.com/>

<https://s.threatbook.cn/>

<https://virusscan.jotti.org>

<http://www.scanvir.com>

<https://app.any.run>

威胁情报

<https://ti.360.net/>

<https://www.venuseye.com.cn/>

<https://x.threatbook.cn/>

<https://redqueen.tj-un.com/IntelHome.html>

<https://exchange.xforce.ibmcloud.com/>

勒索解密

<https://www.osslab.com.tw/nomoreransom/>

<http://lesuobingdu.360.cn/>

<http://www.mottoin.com/tools/96226.html>

<https://www.nomoreransom.org>

<https://ransomwaretracker.abuse.ch/>

<https://noransom.kaspersky.com/>

<https://www.botfrei.de/de/ransomware/galerie.html>

<https://id-ransomware.malwarehunterteam.com/>

<https://www.avast.com/zh-cn/ransomware-decryption-tools>

<http://support.asiainfo-sec.com/Anti-Virus/Clean-Tool/Tools/RansomwareFileDecryptor/>

<https://www.emsisoft.com/decrypter/>

病毒样本

卡饭论坛 : <http://bbs.kafan.cn/>

吾爱破解论坛：<http://www.52pojie.cn/>

看雪：<https://bbs.pediy.com/>

霏凡论坛：<http://bbs.crsky.com/> 要邀请码

爱毒霸社区：<http://bbs.duba.net/forum-3252-1.html>

瑞星卡卡安全论坛：<http://bbs.ikaka.com/showforum-20002.aspx> 要邀请码

伞饭论坛：<http://bbs.sanfans.com/forum.php> 要发贴5

剑盟：<http://bbs.janmeng.com/forum-109-1.html><http://bbs.janmeng.com/forum-109-1.html>

精睿论坛样本测试：<http://bbs.vc52.cn/forum-63-1.html>

动态

CVERC-国家计算机病毒应急处理中心：<http://www.cverc.org.cn>

微步在线威胁情报社区：<https://x.threatbook.cn>

火绒安全论坛：<http://bbs.huorong.cn/forum-59-1.html>

爱毒霸社区：<http://bbs.duba.net>

腾讯电脑管家：<http://bbs.guanjia.qq.com/forum-2-1.html>

相关项目

<https://github.com/hslatman/awesome-threat-intelligence>

<https://github.com/rshipp/awesome-malware-analysis>

<https://github.com/meirwah/awesome-incident-response>