Ferramentas Kali Linux

Aqui fica uma lista das ferramentas que estão presentes no sistema operativo Kali Linux com exemplos.

Estão dispostas como no menu, as que já possuem descrição e exemplos tem uma ligação que pode seguir:
Alguns programas estão repetidos pois tem varias funções e enquadra-se em mais do que um tipo de analise/ataque. Para tal, o mesmo programa pode ter varias ligações sendo cada uma com descrição e exemplos da categoria em que se encontra disposto.

Information Gathering

DNS Analysis

- dnsdict6
- dnsenum
- dnsmap
- dnsrecon
- dnsrevenum6
- dnstracer
- dnswalk
- fierce
- maltego
- nmap
- urlcrazy
- zenmap

IDS/IPS Identification

- fragroute
- fragrouter
- ftest
- lbd
- wafw00f

Live Host identification

- alive6

- cdpsnarf
- detect-new-ip6
- detect_sniffer6
- dmitry
- dnmap-client
- dnmap-server
- fping
- hping3
- inverse_lookup6
- miranda
- ncat
- netdiscover
- nmap
- passive_discovery6
- thcping6
- wol-e
- xprobe2
- zenmap

Network Scanners

- dmitry
- dnmap-client
- dnmap-server
- netdiscover
- nmap
- zenmap

OS Fingerprinting

- dnmap-client
- dnmap-server
- miranda
- nmap
- zenmap

OSINT Analysis

- casefile
- creepy
- dmitry
- jigsaw
- maltego

- theharvester
- twofi
- urlcrazy

Route Analysis

- 0trace
- dnmap-client
- dnmap-server
- intrace
- netmask
- trace6

Service Fingerprinting

- dnmap-client
- dnmap-server
- implementation6
- implementation6d
- ncat
- nmap
- sslscan
- sslyze
- tlssled
- zenmap

SMB Analysis

- acccheck
- nbtscan
- nmap
- zenmap

SMTP Analysis

- nmap
- smtp-user-enum
- swaks
- zenmap

SNMP Analysis

- braa
- cisco-auditing-tool

- copy-router-config
- merge-router-config
- nmap
- onesixtyone
- snmpcheck
- zenmap

SSL Analysis

- sslcaudit
- ssldump
- sslh
- sslscan
- sslsniff
- sslsplit
- sslstrip
- sslyze
- stunnel4
- tlssled

Telephony Analysis

- ace

Traffic Analysis

- 0trace
- cdpsnarf
- ftest
- intrace
- irpas-ass
- irpass-cdp
- p0f
- tcpflow
- wireshark

VoIP Analysis

- ace
- enumiax

VPN Analysis

- ike-scan

Vulnerability Analysis

Cisco Tools

- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- Yersinia

Database Assessment

- bbqsql
- dbpwaudict
- hexorbase
- jsql
- mdb-export
- mdb-hexdump
- mdb-parsecsv
- mdb-sql
- mdb-tables
- oscanner
- sidguesser
- sqldict
- sqlmap
- sqlninja
- sqlsus
- tnscmd10g

Fuzzing Tools

- bed
- fuzz-ip6
- ohrwurm
- powerfuzzer
- sfuzz
- siparmyknife
- spike-generic_chunked
- spike-generic_listen-tcp
- spike-generic_send_tcp
- spike-generic_send_udp

Misc Scanners

- lynis
- nikto
- nmap
- unix-privesc-check
- zenmap

Open Source Assessment

- casefile
- maltego

OpenVAS

- openvas check setup
- openvas feed update
- openvas initial setup
- openvas start
- openvas stop

Web Applications

CMS Identification

- blindelephant
- plecost
- wpscan

Database Exploitation

- bbqsql
- sqlninja
- sqlsus

IDS/IPS Identification

- ua-teste

Web Applications Fuzzers

- burpsuite
- owasp-zap
- powerfuzzer
- webscarab
- webslayer
- websploit

- xsser

Web Applications Proxies

- burpsuite
- owasp-zap
- paros
- proxystrike
- vega
- webscarab

Web Crawlers

- apache-users
- burpsuite
- cutycapt
- dirb
- dirbuster
- owasp-zap
- recon-ng
- vega
- webscarab
- webslayer

Web Vulnerability Scanners

- arachni_web
- burpsuite
- cadaver
- davtest
- deblaze
- fimap
- grabber
- joomscan
- jsql
- nikto
- owasp-zap
- padbuster
- proxystrike
- skipfish
- sqlmap
- uniscan-gui
- vega

- wapiti
- webscarab
- webshag-gui
- websploit
- whatweb
- wpscan
- xsser

Password Attacks

GPU Tools

- cudahashcat-plus
- oclhashcat-lite
- oclhashcat-plus
- pyrit

Offline Attacks

- cachedump
- chntpw
- cmospwd
- crunch
- cudahashcat-plus
- dictstat
- fcrackzip
- hashcat
- hash-identifier
- jonh
- jonhny
- lsadump
- maskgen
- oclhashcat-lite
- oclhashcat-plus
- ophcrack
- ophcrack-client
- policygen
- pwdump
- pyrit
- rainbowcrack
- rcracki_mt

- rsmangler
- samdump2
- sipcrack
- sucrack
- truecrack

Online Attacks

- acccheck
- burpsuite
- cewl
- cisco-auditing-tool
- dbpwaudict
- findmyhash
- hydra
- hydra-gtk
- keimpx
- medusa
- ncrack
- onesistyone
- owasp-zap
- patator
- phrasendrescher
- thc–pptp-bruter
- webscarab

Passing the Hash

- pth-curl
- pth-net
- pth-openchaneclient
- pth-rpcclient
- pth-smbclient
- pth-smbget
- pth-sqsh
- pth-winexe
- pth-wmic
- pth-wmis

Wireless Attacks

802.11. Wireless Tools

- asleap
- bully
- cowpatty
- eapmdpass
- fern-wifi-cracker
- genkeys
- genpmk
- giskismet
- kismet
- mdk3
- wifiarp
- wifidns
- wifi-honey
- wifiping
- wifitap
- wifite

Bluetooth Tools

- bluelog
- bluemaho
- blueranger
- bluesnarfer
- btscanner
- fang
- spooftooph

Other Wireless Tools

- zbassocflood
- zbdsniff
- abdump
- zbfind
- zbgoodfind
- zbreplay
- abstumbler

RFID/NFC Tools

NFC Tools

- mfcuk
- mfoc

- mifare-classic-format
- nfc-list
- nfc-mfclassic

- **RFIDiot ACG**
  - brute force hitag 2
  - bruteforce mifare
  - calculate jcop mifare keys
  - continuos select tag
  - copy iso15693 tag
  - epassport read write clone
  - format mifare 1k value blocks
  - identify hf tag type
  - identify lf tag type
  - jcop info
  - jcop mifare read write
  - jcop set atr historical bytes
  - read acg reader eeprom
  - read lf tag
  - read mifare
  - read tag
  - read write clone unique (em4x02)
  - reset q5 tag
  - select tag
  - set fdx-b id
  - test acg lahf

- RFIDiot FROSCH
  - read write clone unique (em4x02)
  - reset hitag2 tag
  - set fdx-b id
  - test frosch reader

- RFIDiot PCSC
  - bruteforce mifare
  - calculate jcop mifare keys
  - chip & pin info
  - continuos select tag
  - epassport read/write/clone
  - identify hf tag type

- jcop mifare read/write
- jcop set atr historical bytes
- read mifare
- read tag
- select tag

Software Defined Radio

- gnuradio-companion
- gqrx
- gr-scan
- modes_gui
- rtl_adsb
- rtl_fm
- rtl_sdr
- rtlsdr-scanner
- rtl_tcp
- rtl_test

Exploitation Tools

BeEf XSS Framework

- beef

Cisco Attacks

- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- yersinia

Exploit Database

- searchploit

Metasploit

- metasploit community / pro
- metasploit diagnostic logs

- metasploit framework
- update metasploit

Network Exploitation

- armitrage
- exploit6
- ikat
- jboss-autopwn-linux
- jboss-autopwn-win
- termineter

Social Engineering Toolkit

- se-toolkit

Sniffing/Spoofing

Network Sniffers

- darkstat
- dnschef
- dnsspoof
- dnsiff
- ettercap-graphical
- hexinject
- mailsnarf
- msgsnarf
- netsniff-ng
- passive_discovery6
- responder
- sslsniff
- tcpflow
- urlsnarf
- webmitm
- webspy
- wireshark

Network spoofing

- dnschef
- ettercap-graphical
- evilgrade

- fake_dhcps6
- fake_dns6d
- fake_dnsupdate6
- fake_mipv6
- fake_mld26
- fake_mld6
- fake_mldrouter6
- fake_router26
- fake_router6
- fake_solicitate6
- fiked
- macchanger
- parasite6
- randicmp6
- rebind
- redir6
- responder
- sniffjoke
- sslsplit
- sslstrip
- tcpreplay
- wifi-honey
- yersinia

Voice and Surveillance

- msgsnarf

VoIP Tools

- iaxflood
- inviteflood
- ohwurm
- protos-sip
- rtpbreak
- rtpflood
- rtpinsertsound
- rtpmixsound
- sctpscan
- siparmyknife
- sipp
- sipsak

- svmap
- svreport
- svwar
- voiphopper

Web Sniffers

- burpsuite
- dnsspoof
- driftnet
- ferrer
- hamster
- mitmproxy
- owasp-zap
- urlsnarf
- webmitm
- webscarab
- webspy

Maintaing Access

OS Backdoors

- cymothoa
- dbd
- intersect
- powersploit
- sbd
- u3-pwn

Tunneling Tools

- cryptcat
- dbd
- dns2tcpc
- dns2tcpd
- iodine
- miredo
- ncat
- proxychains
- proxytunnel
- ptunnel

- sbd
- socat
- sslh
- stunnel4
- udptunnel

Web Backdoors

- webacoo
- weevely

Reverse Engineering

Debuggers

- edb-debugger
- ollydbg

Disassembly

- jad
- rabin2
- radiff2
- rasm2
- recstudio
- recstudio-cli

Misc RE Tools

- apktool
- clang
- clang++
- dex2jar
- flasm
- javasnoop
- radare2
- rafind2
- ragg2
- ragg2-cc
- rahash2
- rarun2
- rax2

Stress Testing

Network Stress Testing

- denial6
- dhcpig
- dos-new-ip6
- flood_advertise6
- flood_dhcpc6
- flood_mld26
- flood_mld6
- flood_mldrouter6
- flood_router26
- flood_router6
- flood_solicitate6
- fragmentation6
- inundator
- kill_router6
- macof
- rsmurf6
- siege
- smurf6
- t50

VoIP Stress Testing

- iaxflood
- inviteflood

Web Stress Testing

- thc-ssl-dos

WLAN Stress Testing

- mdk3
- reaver

Hardware Hacking

Android Tools

- apktool

- baksmali
- dex2jar
- smali

Arduino Tools

- arduino

Forensics

Anti-virus Forensics Tools

- chkrootkit

Digital Anti-Forensics

- chkrootkit

Digital Forensics

- autospy
- binwalk
- bulk_extractor
- chkrootkit
- dc3dd
- dcfldd
- extundelete
- foremost
- fsstat
- galleta
- tsk_comparedir
- tsk_loaddb

Forensics Analysis Tools

- affcompare
- affcopy
- affcrypto
- affdiskprint
- affinfo
- affsign
- affstats

- affverify
- affxml
- autospy
- binwalk
- blkcalc
- blkcat
- blkstat
- bulk_extractor
- ffind
- fls
- foremost
- galleta
- hfing
- icat-sleuthkit
- ifind
- ils-slethkit
- istat
- jcat
- mactime-sleuthkit
- missidentify
- mmcat
- pdgmail
- readpst
- reglookup
- regripper
- sigfind
- sorter
- srch_strings
- tsk_recover
- vinetto

Forensics Carving Tools

- binwalk
- bulk_extractor
- foremost
- jls
- magicrescue
- pasco
- pev
- recoverjpeg
- rifitui

- safecopy
- scalpel
- scrounge-ntfs

Forensics Hashing Tools

- md5deep
- rahash

Forensics Imaging Tools

- affcat
- affconvert
- blkls
- dc3dd
- dcfldd
- ddrescue
- ewfacquire
- ewfacquirestream
- ewfexport
- ewfinfo
- ewfverify
- fsstat
- guymager
- img_cat
- img_stat
- mmls
- mmstat
- tsk_gettimes

Forensic Suites

- autospy
- dff

Network Forensics

- p0f

Password Forensics Tools

- chntpw

PDF Forensics Tools

- peepdf

RAM Forensics Tools

- volafox
- volatility

Reporting Tools

Documentation

- dradis
- keepnote

Evidence Management

- casefile
- magictree
- maltego
- metagoofil
- pipal
- truecrypt

Media Capture

- cutycapt
- recordmydesktop

System Services

BeEF

- beef start
- beef stop

Dradis

- dradis start
- dradis stop

HTTP

- apache2 restart
- apache2 start
- apache2 stop

Metasploit

- community / pro start
- community / pro stop

MySQL

- mysql restart
- mysql start
- mysql stop

OpenVas

- openvas check setup
- openvas feed update
- openvas initial setup
- openvas start
- openvas stop

SSH

- sshd restart
- sshd start
- sshd stop