www.kali.org /tools/

Kali Tools | Kali Linux Tools

8-10 minutes

- nmap
  - ncat
    - $ ncat
  - ndiff
    - $ ndiff
  - nmap
    - $ nmap
    - $ nping
  - nmap-common

- metasploit-framework
  -
    - $ msf-egghunter
    - $ msf-exe2vba
    - $ msf-exe2vbs
    - $ msf-find_badchars
    - $ msf-halflm_second
    - $ msf-hmac_sha1_crack
    - $ msf-java_deserializer
    - $ msf-jsobfu
    - $ msf-makeiplist
    - $ msf-md5_lookup
    - $ msf-metasm_shell
    - $ msf-msf_irb_shell
    - $ msf-nasm_shell
    - $ msf-pattern_create
    - $ msf-pattern_offset
    - $ msf-pdf2xdp
    - $ msf-virustotal
    - $ msfconsole
    - $ msfd
    - $ msfdb
    - $ msfrpc
    - $ msfrpcd
    - $ msfupdate
    - $ msfvenom

- crunch $

- wireshark
  - libwireshark-data
  - libwireshark-dev
  - libwireshark17t64
  - libwiretap-dev
  - libwiretap14t64
  - libwsutil-dev
  - libwsutil15t64
  - tshark
    - $ tshark
  - wireshark
    - $ wireshark
  - wireshark-common
    - $ capinfos
    - $ captype
    - $ dumpcap
    - $ editcap
    - $ mergecap
    - $ mmdbresolve
    - $ randpkt
    - $ rawshark
    - $ reordercap
    - $ sharkd
    - $ text2pcap
  - wireshark-dev
    - $ asn2deb
    - $ idl2deb
    - $ idl2wrs
  - wireshark-doc

- hashcat
  - hashcat
    - $ hashcat
  - hashcat-data

- hydra
  - hydra
    - $ dpl4hydra
    - $ hydra
    - $ hydra-wizard
    - $ pw-inspector
  - hydra-gtk
    - $ xhydra

- spiderfoot
  -
    - $ spiderfoot
    - $ spiderfoot-cli

- sqlmap
  -
    - $ sqlmap
    - $ sqlmapapi

- nuclei $

- wifite $

- dirb
  -
    - $ dirb
    - $ dirb-gendict
    - $ html2dic

- gobuster $

- hping3 $

- aircrack-ng
  - aircrack-ng
    - $ airbase-ng
    - $ aircrack-ng
    - $ airdecap-ng
    - $ airdecloak-ng

        - $ aireplay-ng
        - $ airmon-ng
        - $ airodump-ng
        - $ airodump-ng-oui-update
        - $ airolib-ng
        - $ airserv-ng
        - $ airtun-ng
        - $ airventriloquist-ng
        - $ besside-ng
        - $ besside-ng-crawler
        - $ buddy-ng
        - $ dcrack
        - $ easside-ng
        - $ ivstools
        - $ kstats
        - $ makeivs-ng
        - $ packetforge-ng
        - $ tkiptun-ng
        - $ wesside-ng
        - $ wpaclean
    - airgraph-ng
        - $ airgraph-ng
        - $ airodump-join

- wpscan $

- netdiscover $

- maltego $

- steghide
    - steghide
        - $ steghide
    - steghide-doc

- mimikatz $

- ettercap
    - ettercap-common
    - ettercap-graphical
        - $ ettercap
        - $ ettercap-pkexec
        - $ etterfilter
        - $ etterlog
    - ettercap-text-only
        - $ ettercap
        - $ etterfilter
        - $ etterlog

- amass
    - amass
        - $ amass
    - amass-common

- theharvester
    -
        - $ restfulHarvest
        - $ theHarvester
        - $ theharvester

- autopsy $

- nikto
    -
        - $ nikto
        - $ replay

- netcat
    - netcat-traditional
        - $ nc.traditional

- burpsuite $

- beef-xss
    -
        - $ beef-xss
        - $ beef-xss-stop

- powershell
    -
        - $ pwsh
        - $ pwsh

- responder
    -
        - $ responder
        - $ responder-BrowserListener
        - $ responder-DHCP_Auto
        - $ responder-FindSQLSrv
        - $ responder-Icmp-Redirect
        - $ responder-MultiRelay
        - $ responder-RunFinger

- snort
    - snort
        - $ appid_detector_builder.sh
        - $ snort
        - $ snort2lua
        - $ u2boat
        - $ u2spewfoo
    - snort-common
    - snort-common-libraries
    - snort-doc
    - snort-rules-default

- john
    - john
        - $ SIPdump
        - $ base64conv
        - $ bitlocker2john
        - $ calc_stat
        - $ cprepair
        - $ dmg2john
        - $ eapmd5tojohn
        - $ genmkvpwd
        - $ gpg2john
        - $ hccap2john
        - $ john
        - $ keepass2john
        - $ mailer
        - $ mkvcalcproba
        - $ putty2john
        - $ racf2john

    - $ rar2john
    - $ raw2dyna
    - $ tgtsnarf
    - $ uaf2john
    - $ unafs
    - $ undrop
    - $ unique
    - $ unshadow
    - $ vncpcap2john
    - $ wpapcap2john
    - $ zip2john
- john-data
    - $ 1password2john
    - $ 7z2john
    - $ DPAPImk2john
    - $ adxcsouf2john
    - $ aem2john
    - $ aix2john
    - $ andotp2john
    - $ androidbackup2john
    - $ androidfde2john
    - $ ansible2john
    - $ apex2john
    - $ applenotes2john
    - $ aruba2john
    - $ atmail2john
    - $ axcrypt2john
    - $ bestcrypt2john
    - $ bitcoin2john
    - $ bitshares2john
    - $ bitwarden2john
    - $ bks2john
    - $ blockchain2john
    - $ ccache2john
    - $ cisco2john
    - $ cracf2john
    - $ dashlane2john
    - $ deepsound2john
    - $ diskcryptor2john
    - $ dmg2john
    - $ ecryptfs2john
    - $ ejabberd2john
    - $ electrum2john
    - $ encfs2john
    - $ enpass2john
    - $ enpass5tojohn
    - $ ethereum2john
    - $ filezilla2john
    - $ geli2john
    - $ hccapx2john
    - $ htdigest2john
    - $ ibmiscanner2john
    - $ ikescan2john
    - $ ios7tojohn
    - $ itunes_backup2john
    - $ iwork2john
    - $ kdcdump2john
    - $ keychain2john
    - $ keyring2john
    - $ keystore2john
    - $ kirbi2john
    - $ known_hosts2john
    - $ krb2john
    - $ kwallet2john
    - $ lastpass2john
    - $ ldif2john
    - $ libreoffice2john
    - $ lion2john
    - $ lotus2john
    - $ luks2john
    - $ mac2john
    - $ mcafee_epo2john
    - $ monero2john
    - $ money2john
    - $ mosquitto2john
    - $ mozilla2john
    - $ multibit2john
    - $ neo2john
    - $ office2john
    - $ openbsd_softraid2john
    - $ openssl2john
    - $ padlock2john
    - $ pcap2john
    - $ pdf2john
    - $ pem2john
    - $ pfx2john
    - $ pgpdisk2john
    - $ pgpsda2john
    - $ pgpwde2john
    - $ prosody2john
    - $ ps_token2john
    - $ pse2john
    - $ pwsafe2john
    - $ radius2john
    - $ restic2john
    - $ sap2john
    - $ sense2john
    - $ signal2john
    - $ sipdump2john
    - $ ssh2john
    - $ sspr2john
    - $ staroffice2john
    - $ strip2john
    - $ telegram2john
    - $ tezos2john
    - $ truecrypt2john
    - $ vdi2john
    - $ vmx2john
    - $ zed2john

- rkhunter $
- ffuf $
- macchanger $

- cisco-torch $
- tcpdump $
- bloodhound $
- lynis $
- yersinia $
- dirbuster $
- cewl
  - $ cewl
  - $ fab-cewl
- armitage
  - $ armitage
  - $ teamserver
- airgeddon $
- above $
- wifiphisher $
- veil
  - veil
    - $ veil
  - veil-catapult
  - veil-evasion
- recon-ng
  - $ recon-cli
  - $ recon-ng
  - $ recon-web
- dnsrecon $
- dnsenum $
- zenmap-kbx $
- whatweb $
- scapy
  - python3-scapy
    - $ scapy
    - $ scapy3
- reaver
  - $ reaver
  - $ wash
- parsero $
- dsniff
  - $ arpspoof
  - $ dnsspoof
  - $ dsniff
  - $ filesnarf
  - $ macof
  - $ mailsnarf
  - $ msgsnarf
  - $ sshmitm
  - $ sshow
  - $ tcpkill
  - $ tcpnice
  - $ urlsnarf
  - $ webmitm
  - $ webspy
- arpwatch
  - $ arp2ethers
  - $ arpfetch
  - $ arpsnmp
  - $ arpwatch
  - $ bihourly
  - $ massagevendor
- sherlock $
- netexec
  - $ netexec
  - $ nxc
  - $ nxcdb
- legion $
- lbd $
- kismet
  - kismet
  - kismet-capture-common
  - kismet-capture-hak5-wifi-coconut
    - $ kismet_cap_hak5_wifi_coconut
  - kismet-capture-linux-bluetooth
    - $ kismet_cap_linux_bluetooth
  - kismet-capture-linux-wifi
    - $ kismet_cap_linux_wifi
  - kismet-capture-nrf-51822
    - $ kismet_cap_nrf_51822
  - kismet-capture-nrf-52840
    - $ kismet_cap_nrf_52840
  - kismet-capture-nrf-mousejack
    - $ kismet_cap_nrf_mousejack
  - kismet-capture-nxp-kw41z
    - $ kismet_cap_nxp_kw41z
  - kismet-capture-rz-killerbee
    - $ kismet_cap_rz_killerbee
  - kismet-capture-ti-cc-2531
    - $ kismet_cap_ti_cc_2531
  - kismet-capture-ti-cc-2540
    - $ kismet_cap_ti_cc_2540
  - kismet-capture-ubertooth-one
    - $ kismet_cap_ubertooth_one
  - kismet-core
    - $ kismet

        - $ kismet_cap_kismetdb
        - $ kismet_cap_pcapfile
        - $ kismet_server
    - kismet-logtools
        - $ kismetdb_clean
        - $ kismetdb_dump_devices
        - $ kismetdb_statistics
        - $ kismetdb_strip_packets
        - $ kismetdb_to_gpx
        - $ kismetdb_to_kml
        - $ kismetdb_to_pcap
        - $ kismetdb_to_wiglecsv
    - kismet-plugins
        - $ kismet_discovery
        - $ kismet_eventbus
        - $ kismet_proxytest
    - python3-kismetcapturebtgeiger
        - $ kismet_cap_bt_geiger
    - python3-kismetcapturefreaklabszigbee
        - $ kismet_cap_freaklabs_zigbee
    - python3-kismetcapturertl433
        - $ kismet_cap_sdr_rtl433
    - python3-kismetcapturertladsb
        - $ kismet_cap_sdr_rtladsb
    - python3-kismetcapturertlamr
        - $ kismet_cap_sdr_rtlamr

- impacket-scripts
    -
        - $ impacket-DumpNTLMInfo
        - $ impacket-Get-GPPPassword
        - $ impacket-GetADUsers
        - $ impacket-GetNPUsers
        - $ impacket-GetUserSPNs
        - $ impacket-addcomputer
        - $ impacket-atexec
        - $ impacket-changepasswd
        - $ impacket-dcomexec
        - $ impacket-dpapi
        - $ impacket-esentutl
        - $ impacket-exchanger
        - $ impacket-findDelegation
        - $ impacket-getArch
        - $ impacket-getPac
        - $ impacket-getST
        - $ impacket-getTGT
        - $ impacket-goldenPac
        - $ impacket-karmaSMB
        - $ impacket-keylistattack
        - $ impacket-kintercept
        - $ impacket-lookupsid
        - $ impacket-machine_role
        - $ impacket-mimikatz
        - $ impacket-mqtt_check
        - $ impacket-mssqlclient
        - $ impacket-mssqlinstance
        - $ impacket-net
        - $ impacket-nmapAnswerMachine
        - $ impacket-ntfs-read
        - $ impacket-ntlmrelayx
        - $ impacket-ping
        - $ impacket-ping6
        - $ impacket-psexec
        - $ impacket-raiseChild
        - $ impacket-rbcd
        - $ impacket-rdp_check
        - $ impacket-reg
        - $ impacket-registry-read
        - $ impacket-rpcmap
        - $ impacket-sambaPipe
        - $ impacket-services
        - $ impacket-smbclient
        - $ impacket-smbexec
        - $ impacket-smbpasswd
        - $ impacket-smbrelayx
        - $ impacket-smbserver
        - $ impacket-sniff
        - $ impacket-sniffer
        - $ impacket-split
        - $ impacket-ticketConverter
        - $ impacket-ticketer
        - $ impacket-tstool
        - $ impacket-wmipersist
        - $ impacket-wmiquery

- havoc $

- dirsearch $

- crackmapexec
    -
        - $ cmedb
        - $ crackmapexec

- chntpw
    -
        - $ chntpw
        - $ reged
        - $ sampasswd
        - $ samunlock
        - $ samusrgrp

- wordlists $

- ghidra $

- foremost $

- fcrackzip
    -
        - $ fcrackzip
        - $ fcrackzipinfo

- eyewitness
    -
        - $ eyewitness
        - $ geckodriver

- evil-winrm $

- enum4linux $

- cryptsetup
  - cryptsetup
    - $ cryptdisks_start
    - $ cryptdisks_stop
    - $ luksformat
  - cryptsetup-bin
    - $ cryptsetup
    - $ integritysetup
    - $ veritysetup
  - cryptsetup-initramfs
  - cryptsetup-ssh
    - $ cryptsetup-ssh
  - cryptsetup-suspend
  - libcryptsetup-dev
  - libcryptsetup12
- chkrootkit
  -
    - $ chklastlog
    - $ chkrootkit
    - $ chkrootkit-daily
    - $ chkwtmp
- binwalk
  - binwalk
    - $ binwalk
  - python3-binwalk
- bettercap $
- yara
  - libyara-dev
  - libyara10
  - yara
    - $ yara
    - $ yarac
  - yara-doc
- trufflehog
  -
    - $ snifftest
    - $ trufflehog
    - $ trufflehog-generate
- subfinder $
- sparrow-wifi
  -
    - $ sparrow-wifi
    - $ sparrowwifiagent
- shellter $
- set
  -
    - $ se-toolkit
    - $ setoolkit
- nbtscan $
- masscan $
- httrack
  - httrack
    - $ httrack
  - httrack-doc
  - libhttrack-dev
  - libhttrack2
  - proxytrack
    - $ proxytrack
  - webhttrack
    - $ htsserver
    - $ webhttrack
  - webhttrack-common
- gophish
  -
    - $ gophish
    - $ gophish-stop
- goldeneye $
- firewalk $
- fierce $
- dmitry $
- chisel $
- xsser $
- wifipumpkin3
  -
    - $ captiveflask
    - $ evilqr3
    - $ phishkin3
    - $ sslstrip3
    - $ wifipumpkin3
    - $ wp3
- wfuzz $
- wafw00f $
- sublist3r $
- socat
  -
    - $ filan
    - $ procan
    - $ socat
    - $ socat-broker.sh
    - $ socat-chain.sh
    - $ socat-mux.sh
    - $ socat1
- smbmap $
- skipfish $