Senarai Perangkat Keamanan Informasi di Kali Linux

Happy Chandraleka, S.T.
Pranata Komputer di Pusat Kebijakan
Sistem Ketahanan Kesehatan dan Sumber
Daya Kesehatan, Kementerian Kesehatan RI.

Senarai
Perangkat Keamanan Informasi
pada Kali Linux

Oleh Happy Chandraleka, S.T.
Pranata Komputer di Pusat Kebijakan Sistem Ketahanan Kesehatan dan Sumber Daya Kesehatan, Kementerian Kesehatan RI.
Ditulis di Jakarta 07 Juni 2024 M

Kali Linux merupakan distribusi Linux yang dikhususkan untuk *digital forensics* dan *penetration testing*. Dibangun oleh Offensive Security, sebuah perusahaan internasional yang berbasis di Amerika dengan lingkup usaha mengenai *information security, penetration testing dan digital forensics*. Kali Linux versi *full* setidaknya memuat 600an perangkat keamanan informasi. Distribusi Kali Linux sendiri dibangun berdasarkan Debian dan sebagian besar repositorinya berasal dari Debian.

Menurut Hasan Rizky Putra Sailellah (https://it.telkomuniversity.ac.id/kali-linux-pengertian-sejarah-kelebihan-kekurangan-jenisnya/) Kali Linux memuat kelebihan dan kekurangan seperti dijelaskan berikut ini.

Kelebihan

- Terintegrasi dengan berbagai alat keamanan: Kali Linux memiliki lebih dari 600 alat keamanan yang terintegrasi, seperti Nmap, Wireshark, Metasploit, dan Aircrack-ng, yang dapat membantu pengguna dalam melakukan tes penetrasi dan pengujian keamanan.
- Gratis dan Open Source: Kali Linux tersedia secara gratis dan open source, sehingga siapa pun dapat mengunduh dan menggunakannya tanpa membayar lisensi.
- Kompatibilitas hardware yang baik: Kali Linux dapat diinstal pada berbagai jenis hardware dan kompatibel dengan berbagai perangkat keras.

- Memiliki komunitas yang besar: Kali Linux memiliki komunitas pengguna yang besar dan aktif yang membantu dalam memberikan dukungan dan solusi jika terjadi masalah pada sistem.

Kekurangan

- Tidak cocok untuk pengguna pemula: Kali Linux dirancang khusus untuk ahli keamanan dan profesional TI yang memahami keamanan jaringan dan sistem, sehingga pengguna pemula mungkin kesulitan dalam mengoperasikan dan menguji sistem.
- Kurangnya dukungan resmi: Kali Linux tidak didukung secara resmi oleh vendor perangkat lunak atau perusahaan tertentu, sehingga mungkin sulit untuk mendapatkan dukungan teknis jika terjadi masalah atau kesalahan.
- Kurang stabil: Kali Linux sering mendapatkan pembaruan, sehingga mungkin kurang stabil dan sering mengalami bug atau kesalahan.

Meskipun Kali Linux memiliki beberapa kekurangan, tetapi kelebihannya yang menonjol dalam bidang keamanan menjadikannya pilihan populer bagi para profesional dan pengguna yang membutuhkan sistem operasi untuk pengujian keamanan.

Berikut ini daftar perangkat keamanan informasi pada Kali Linux.

01 Information Gathering

- DNS Analysis
    - Dnsenum
    - Dnsmap
    - Dnsrecon
    - fierce
- IDS/IPS Identification
    - Lbd
    - Wafw00f
- Live Host Identification
    - Arping
    - Fping
    - Hping3
    - Masscan
    - Netcat
    - Thcping6
    - unicornscan
- Network & Port Scanners
    - Masscan
    - Nmap

    - unicorn
- OSINT Analysis
    - Maltego
    - Spiderfoot
    - Spiderfoot-cli
    - theharvester
- Route Analysis
    - Netdiscover
    - netmask
- SMB Analysis
    - Enum4linux
    - Nbtscan
    - smbmap
- SMTP Analysis
    - Smtp-user-enum
    - Swaks
- SNMP Analysis
    - Onesixtyone
    - Snmp-check
- SSL Analysis
    - Ssldump
    - Sslh
    - sslyze
- Amass
- Dmitry
- Ike-scan
- Legion
- Maltego
- Netdiscover
- Nmap
- Recon-ng
- spiderfoot

02 Vulnerability Analysis

- Fuzzing Tools
    - Spike-generic_chunked
    - Spike-generic_listen_tcp
    - Spike-generic_send_tcp
    - Spike-generic_send_udp
- VoIP Tools
    - voiphopper
- Legion

- Nikto
- Nmap
- Unix-privesc-check

03 Web Application Analysis

- CMS & Framework Identification
    - wpscan
- Web Application Proxies
    - burpsuite
- Web Crawlers & Directory Brut
    - Cutycapt
    - Dirb
    - Dirbuster
    - Ffuf
    - wfuzz
- Web Vulnerability Scanners
    - Cadaver
    - Davtest
    - Nikto
    - Skipfish
    - Wapiti
    - Whatweb
    - Wpscan
- Burpsuite
- Commix
- Skipsifh
- Sqlmap
- Webshells
- Wpscan

04 Database Assessment

- SQLite database browser
- Sqlmap

05 Password Attacks

- Offline Attacks
    - Chntpw
    - Hashcat

    - Hashid
    - Hash-identifier
    - John
    - Ophcrack-cli
    - Samdump2
- Online Attacks
    - Hydra
    - Hydra-graphical
    - Medusa
    - Ncrack
    - Onesixtyone
    - Patator
    - Thc-pptp-bruter
- Passing the Hash Tools
    - Crackmapexec
    - Evil-winrm
    - Impacket
    - Mimikatz
    - Pth-curl
    - Pth-net
    - Pth-rpcclient
    - Pth-smbclient
    - Pth-smbget
    - Pth-sqsh
    - Pth-winexe
    - Pth-wmic
    - Pth-wmis
    - Pthxfreerdp
    - smbmap
- Password Profiling & Wordlists
    - Cewl
    - Cruch
    - Rsmangler
    - Wordlists
- Cewl
- Crunch
- Hashcat
- Hydra
- John
- Medusa
- Ncrack
- Ophcrack
- Wordlists

06 Wireless Attacks

- 802.11 Wireless Tools
    - Bully
    - Fern wifi cracker (root)
- Bluetooth Tools
    - spooftooph
- Aircrack-ng
- Fern wifi cracker (root)
- Kismet
- Pixiewps
- Reaver
- wifite

07 Reverse Engineering

- clang
- clang++
- NASM shell
- Radare2

08 Exploitation Tools

- Crackmapexec
- Metasploit framework
- Msf payload creator
- Searchsploit
- Social engineering toolkit (root)
- sqlmap

09 Sniffing & Spoofing

- Network Sniffers
    - Dnschef
    - Dsniff
    - Netsniff-ng
- Spoofing & MITM
    - Dnschef
    - Rebind
    - Sslsplit

    - tcpreplay
- Ettercap-graphical
- Macchanger
- Minicom
- Mitmproxy
- Netsniff-ng
- Responder
- Scapy
- Tcpdump
- Wireshark

10 Post Exploitation

- OS Backdoors
    - Dbd
    - Powersploit
    - sbd
- Tunneling & Exfiltration
    - Dbd
    - Dns2tcpc
    - Dns2tcpd
    - Exe2hex
    - Iodine
    - Miredo
    - Proxychains4
    - Proxytunnel
    - Ptunnel
    - Pwnat
    - Sslh
    - Stunnel4
    - udptunnel
- Web Backdoors
    - Laudanum
    - weevely
- Evil-winrm
- Exe2hex
- Impacket
- Mimikatz
- Netcat
- Powershell empire
- Powersploit
- Proxychains4
- Starkiller

- Weevely

11 Forensics

- Forensic Carving Tools
  - Magicrescue
  - Scalpel
  - Scrounge-ntfs
- Forensic Imaging Tools
  - Guymager (root)
- PDF Forensics Tools
  - Pdfid
  - Pdf-parser
- Sleuth Kit Suite
  - Autopsy (root)
  - Blkcalc
  - Blkcat
  - Blkls
  - Blkstat
  - Ffind
  - Fls
  - Fsstat
  - Hfind
  - Icat-sleuthkit
  - Ifind
  - Ils-sleuthkit
  - Img_cat
  - Img_stat
  - Istat
  - Jcat
  - Jls
  - Mactime-sleuthkit
  - Mmcat
  - Mmls
  - Mmstat
  - Sigfind
  - Sorter
  - Srch_strings
  - Tsk_comparedir
  - Tsk_gettimes
  - Tsk_loaddb
  - Tsk_recover
- Autopsy (root)

- Binwalk
- Bulk_extractor
- Hashdeep

12 Reporting Tools

- CherryTree
- Cutycapt
- Faraday start
- Maltego
- Pipal
- Recordmydesktop

13 Social Engineering Tools

- Maltego
- Msf payload creator
- Social engineering toolkit (root)

42 Kali & Offset Links

- Exploit Database
- Kali Bugs
- Kali Docs
- Kali Forums
- Kali Linux
- Kali Tools
- NetHunter
- Offset Training
- VulnHub

Senarai Perangkat Keamanan Informasi di Kali Linux

Kali Linux merupakan distribusi Linux yang dikhususkan untuk *digital forensics* dan *penetration testing*. Dibangun oleh Offensive Security, sebuah perusahaan internasional yang berbasis di Amerika dengan lingkup usaha mengenai *information security, penetration testing dan digital forensics*. Kali Linux versi *full* setidaknya memuat 600an perangkat keamanan informasi. Distribusi Kali Linux sendiri dibangun berdasarkan Debian dan sebagian besar repositorinya berasal dari Debian.

Buku ini memuat daftar perangkat keamanan informasi yang ada di Kali Linux. Silahkan menyimak.