
KALI
BY OFFENSIVE SECURITY

Kali Linux არის Linux დისტრიბუცია, რომლის პროგრამული უზრუნველყოფა დაფუძნებულია Debian Testing ფილიალზე: Kali პაკეტების უმეტესობა იმპორტირებულია Debian საცავებიდან.

- ✓ **Initial release:** 2013 წელი, 13 მარტი
- ✓ **latest release:** 2024 წლის 11 სექტემბერი
- ✓ **Mati Aharoni, Devon Kearns**

- პირველი ვერსია, 1.0.0 "moto", გამოვიდა 2013 წლის მარტში.

- 2019.4 ვერსიით 2019 წლის ნოემბერში, ნაგულისხმევი მომხმარებლის ინტერფეისი გადავიდა GNOME-დან Xfce-ზე, GNOME-ის ვერსია ჯერ კიდევ ხელმისაწვდომია.

- 2020.3 ვერსიით 2020 წლის აგვისტოში, ნაგულისხმევი გარსი გადაერთო Bash-დან ZSH-ზე, ხოლო Bash დარჩა როგორც ოფცია.

Kali Linux-ს აქვს დაახლოებით 600 შეღწევადობის ტესტირების პროგრამა (ინსტრუმენტები), მათ შორის :

- **Armitage** (გრაფიკული კიბერშეტევების მართვის ინსტრუმენტი),
- **Nmap** (პორტის სკანერი),
- **Wireshark** (პაკეტების ანალიზატორი),
- **metasploit** (შეღწევადობის ტესტირების ჩარჩო),
- **ohn the Ripper** (პაროლის კრეკერი),
- **sqlmap** (ავტომატური **SQL** ინექციის და მონაცემთა ბაზის აღების ინსტრუმენტი),
- **Aircrack-ng** (პროგრამული კომპლექტი უსადენო **LAN**-ების შეღწევადობის ტესტირებისთვის),
- **OWASP ZAP** ვებ აპლიკაციის უსაფრთხოების სკანერები...

Kali Linux შემუშავებულია
კიბერუსაფრთხოების
ექსპერტების, შეღწევადობის
ტესტერებისა და
ე.წ ჰაკერების მიმართ.
არსებობს რამდენიმე სხვა დისტრიბუცია,
რომელიც ემღვნება შეღწევადობის ტესტირებ
როგორიცაა Parrot OS,
BlackArch და Wifislax. Kali Linux გამოირჩეოდა ად
დისტრიბუციების წინააღმდეგ
კიბერუსაფრთხოების და
შეღწევადობის
ტესტირებისთვის,
ასევე აქვს სუპერმომხმარებელის შექმნის
ფუნქცია Kali Live Environment-ში.

Supported platforms

- Asus Chromebook Flip C100P,
- BeagleBone Black,
- HP Chromebook,
- CubieBoard 2,
- CuBox,
- CuBox-i,
- Raspberry Pi,
- EfikaMX,
- Odroid U2,
- Odroid XU,
- Odroid XU3,
- Samsung Chromebook,
- Utilite Pro,
- Galaxy Note 10.1,
- SS808.[18]


REQUIREMENT

- მინიმუმ 20 GB ადგილი მყარ დისკზე ინსტალაციისთვის, ვერსიის მიხედვით.
- მინიმუმ 2 GB ოპერატიული მეხსიერება i386 და AMD64 არქიტექტურისთვის.
- ჩამტვირთავი CD-DVD დისკი ან USB დისკი.
- მინიმუმ Intel Core i3 ან AMD E1 პროცესორი კარგი მუშაობისთვის.
- 50 GB ადგილი მყარ დისკზე, სასურველია SSD.
- მინიმუმ 2 GB ოპერატიული მეხსიერება.

security tools

- Aircrack-ng
- Autopsy
- Armitage
- Burp Suite
- BeEF
- Cisco Global Exploiter
- Ettercap
- Foremost
- Hydra
- Hashcat
- John the Ripper
- Kismet
- Lynis
- Maltego
- Metasploit framework
- Nmap
- Nikto
- OWASP ZAP
- Reverse engineering toolkit
- Social engineering tools
- Sqlmap
- Volatility
- VulnHub
- Wireshark
- WPScan


NMAP
HASHCAT
JOHN THE RIPPER
Burp Suite
AIRCRACK-NG
Kali Linux Tools

ეს ხელსაწყოები შეიძლება გამოყენებულ იქნას მრავალი მიზნისთვის, რომელთა უმეტესობა მოიცავს ქსელის ან აპლიკაციის ექსპლუატაციას, ქსელის აღმოჩენისს ან სამიზნე IP მისამართის სკანირებას. მრავალი ინსტრუმენტი წინა ვერსიიდან (BackTrack) აღმოიფხვრა, რათა ფოკუსირდნენ შეღწევადობის ტესტირების ყველაზე პოპულარულ და ეფექტურ აპლიკაციებზე.

ანი მაისურაძე
ჯგუფი 6