**LINUX TOOLS**

**Nmap**: Tarmoqni skanerlash va portlarni tekshirish uchun ishlatiladi.​

**Nmap – Tarmoq va portlarni skanerlash**

* **Maqsadi:** Tarmoqdagi qurilmalarni aniqlash, portlarni tekshirish va zaifliklarni topish.
* nmap <IP> # Oddiy skan
* nmap -sS <IP> # Yashirin SYN skan
* nmap -O <IP> # Operatsion tizimni aniqlash
* nmap -A <IP> # Kengaytirilgan skan (OS, versiyalar, skriptlar)

**Netcat**: Tarmoq ulanishlarini o'qish va yozish, portlarni skanerlash va fayllarni uzatish uchun ishlatiladi.​

**Netcat (nc) – Tarmoq ulanishlarini sinovdan o'tkazish**

* **Maqsadi:** Server va portlarni tekshirish, ma'lumot uzatish, teskari shell ochish.
* nc -lvnp 4444 # Port tinglash
* nc <IP> 4444 # Masofaviy ulanish
* nc -zv <IP> 80-100 # 80-100 portlarni skanerlash

**Fluxion** – Wi-Fi xavfsizligini tekshirish vositasi

Fluxion **Wi-Fi tarmoqlari himoyasini tekshirish** va **ijtimoiy muhandislik hujumlarini o‘rganish** uchun ishlatiladi.

* git clone <https://github.com/FluxionNetwork/fluxion.git>
* cd fluxion
* ./fluxion.sh
* airmon-ng start wlan0
* ./fluxion.sh

**Lynis** – Tizim xavfsizligini tekshirish vositasi.

Lynis **tizim xavfsizligini mustahkamlash** va **zaifliklarni aniqlash** uchun ishlatiladi. Uni **IT xavfsizlik mutaxassislari**, **dasturchilar** va **tizim administratorlari** ishlatishadi.

* sudo lynis audit system

**Nessus** – Zaifliklarni aniqlash vositasi.

Nessus **tizim va dasturlar zaifliklarini aniqlash**, **noto‘g‘ri sozlamalarni tekshirish**, hamda **potensial tahdidlarni topish** uchun ishlatiladi. IT xavfsizlik mutaxassislari va tizim administratorlari undan foydalanishadi.

**Tiger**: Xavfsizlik auditi va xost tomonidagi buzilishlarni aniqlash uchun ishlatiladigan buyruq satri vositasi.​[totrdlo.ru](https://totrdlo.ru/uz/kali-linux-obzor-programm-luchshie-instrumenty-kali-linux-kali-linux-izmeneniya-v-novoi.html?utm_source=chatgpt.com)

**John the Ripper**: Parol xavfsizligini tekshirish va parollarni tiklash uchun ishlatiladigan parol buzish vositasi.

**John the Ripper – Parollarni sinash va buzish**

* **Maqsadi: Hashlangan parollarni yechish.**
* **john --wordlist=rockyou.txt hashes.txt # Parolni sinash**
* **john --show hashes.txt # Buzilgan parollarni ko'rsatish**

**Hydra**: Ko'p protokollar bo'yicha parallel ulanishlar va hujumlarni amalga oshiruvchi parol buzish vositasi.​

**Hydra – Brute-force (majburiy kalit topish) hujumi**

* **Maqsadi:** SSH, FTP, va boshqa autentifikatsiya tizimlariga kuchli parollarni sinash.
* hydra -l admin -P passwords.txt 192.168.1.1 ssh # SSH brute-force
* hydra -L users.txt -P pass.txt ftp://192.168.1.1 # FTP brute-force

**Social-Engineer Toolkit (SET)**: Ijtimoiy muhandislik tadqiqotlari uchun mo'ljallangan penetratsion test to'plami.​[totrdlo.ru+1uz.linux-console.net+1](https://totrdlo.ru/uz/kali-linux-obzor-programm-luchshie-instrumenty-kali-linux-kali-linux-izmeneniya-v-novoi.html?utm_source=chatgpt.com)

**WPScan**: WordPress veb-saytlaridagi zaifliklarni, noto'g'ri konfiguratsiyalarni va xavfsizlik muammolarini aniqlash uchun ishlatiladi.​

**Metasploit Framework**: Penetratsion test tizimi va ekspluatatsiya vositalarini yaratish platformasi.​[uz.linux-console.net](https://uz.linux-console.net/?p=27776&utm_source=chatgpt.com)

**Metasploit Framework – Ekspluatatsiya va sinov hujumlari**

* **Maqsadi:** Tizimdagi zaifliklarni aniqlash va ekspluatatsiya qilish.
* msfconsole # Metasploit'ni ishga tushirish
* search exploit windows # Windows ekspluatlarini qidirish
* use exploit/multi/handler # Ekspluatni tanlash
* set payload windows/meterpreter/reverse\_tcp # Payload o'rnatish
* exploit # Hujumni boshlash

**Burp Suite**: Veb-ilovalarni xavfsizlik bo'yicha sinovdan o'tkazish va zaifliklarni aniqlash uchun platforma.​[Vikipediya](https://uz.wikipedia.org/wiki/Kali_Linux?utm_source=chatgpt.com)

**Burp Suite – Web ilovalari zaifliklarini tahlil qilish**

* **Maqsadi:** XSS, SQL Injection kabi zaifliklarni toppish.
* burpsuite

**Aircrack-ng**: Wi-Fi tarmoqlarining xavfsizligini baholash, tarmoq trafigini tahlil qilish va parollarni buzish uchun ishlatiladi.

**10. Aircrack-ng – Wi-Fi himoyasini buzish va tahlil qilish**

* **Maqsadi:** WEP va WPA2 parollarini buzish.
* airmon-ng start wlan0 # Monitor rejimini yoqish
* airodump-ng wlan0mon # Tarmoqni skanerlash
* aircrack-ng capture.cap -w wordlist.txt # Parolni buzish

**Nikto**: Veb-serverlar va ilovalarni zaifliklar uchun skanerlash vositasi.​

**Nikto – Web server skaneri**

* **Maqsadi:** Web-serverlardagi zaifliklarni aniqlash.
* nikto -h <http://example.com>

**Autopsy Forensic Browser:** Raqamli qurilmalardan ma'lumotlarni olish va tahlil qilish uchun raqamli kriminalistika vositasi.​

**King Phisher:** Fishing kampaniyalarini simulyatsiya qilish va xavfsizlik bo'yicha xabardorlikni oshirish uchun ishlatiladi.​

**Skipfish**: Veb-ilovalarni xavfsizlik bo'yicha baholash va zaifliklarni aniqlash uchun vosita.​

**Browser Exploitation Framework (BeEF):** Veb-brauzerlarning zaifliklarini sinovdan o'tkazish va baholash uchun platforma.​

**Wireshark:** Tarmoq trafigini real vaqtda tahlil qilish va tarmoq muammolarini aniqlash uchun paket tahlilchisi.​

**Wireshark – Tarmoq tahlili va paket sniffingi**

* **Maqsadi:** Tarmoq trafikini ko'rish va tahlil qilish.
* wireshark # GUI interfeysni ishga tushirish
* tshark -i wlan0 # Terminalda trafikni kuzatish
* tshark -r capture.pcap # Oldin yozib olingan paketlarni tahlil qilish

**Yersinia:** Tarmoq protokollariga hujumlarni simulyatsiya qilish va sinovdan o'tkazish uchun vosita.​

**Maltego:** Turli manbalardan ma'lumotlarni yig'ish va tahlil qilish uchun intellekt va ma'lumotlarni vizualizatsiya qilish vositasi.​

**Apktool:** Android APK fayllarini teskari muhandislik qilish va tahlil qilish uchun vosita.​

**Sqlmap:** Veb-ilovalardagi SQL in'ektsiya zaifliklarini aniqlash va ekspluatatsiya qilish uchun avtomatlashtirilgan vosita.​

**Dirb**: Veb-serverlardagi yashirin yoki himoyalanmagan kataloglar va fayllarni aniqlash uchun brute-force vositasi.​

**Reaver – WPS zaifliklarini ekspluatatsiya qilish**

* **Maqsadi:** WPS orqali Wi-Fi parollarini buzish.
* reaver -i wlan0mon -b [BSSID] -vv