

# Инструменты для инженера ИБ и этичного хакера

## 1. Text Editors & IDE

- VS Code: Универсальный редактор, куча расширений
- CLion: Разработка на C/C++ (в т.ч. для Linux/Android)
- IntelliJ IDEA: Java, Kotlin, Python, web-проекты
- Android Studio: Android reverse, Java/C++ (NDK)
- Visual Studio: Разработка под Windows, анализ PE-файлов
- Vim / Neovim: Лёгкий CLI-редактор, удобен для RE и pentest

## 2. Терминал и окружение

- Bash/Zsh/Fish: Скрипты, автоматизация, конфиги
- tmux/screen: Множественные сессии, удалённая работа
- ssh/rsync: Подключение, копирование
- curl/wget: Быстрые HTTP-запросы
- htop/nmon: Мониторинг системы

## 3. Reverse Engineering

- Ghidra: Реверс ELF/PE, cross-platform
- IDA Free/Pro: Лучший дизассемблер (но платный)
- Radare2 / Cutter: CLI + GUI альтернатива IDA
- Apktool / JADX: Анализ .apk, декомпиляция Java
- Frida: Hook'и в рантайме для Android и iOS
- x64dbg / OllyDbg: Windows-дебаггеры

## 4. Pentest / Exploitation

- Metasploit: Эксплойты, payload'ы, post-exploitation
- Empire / Covenant: Red team инструменты на PowerShell/C#
- Cobalt Strike: Коммерческий Red Team toolkit
- Exploit-DB / Searchsploit: База известных эксплойтов

## 5. Сканеры и анализаторы

- nmap: Скан портов и сервисов

## Инструменты для инженера ИБ и этичного хакера

- masscan: Очень быстрый порт-сканер
- Nikto: Сканер веб-уязвимостей
- wpscan: WordPress анализатор
- whatweb: Определение технологий сайта

### 6. Web Pentest

- Burp Suite: Ловец HTTP-трафика, пентест сайтов
- OWASP ZAP: Open Source аналог Burp
- SQLmap: SQL-инъекции
- XSS-Scanner: Поиск XSS уязвимостей
- dirsearch / gobuster / ffuf: Brute-force директорий и URL

### 7. Трафик и sniffing

- Wireshark: Анализ сетевых пакетов
- tcpdump: CLI альтернатива Wireshark
- mitmproxy: MITM HTTP/HTTPS прокси
- ettercap / arpspoof: ARP-spoofing и MITM

### 8. Android/iOS hacking

- ADB / fastboot: Подключение, дамп, управление Android
- MobSF: Статический и динамический анализ APK
- Frida: Hook'и в рантайме
- Drozer: Поиск уязвимостей в Android-приложениях
- apktool / jadx: Декомпиляция и пересборка .apk

### 9. Среда для тестов

- VirtualBox / VMware / QEMU: Песочницы для тестов
- Docker: Деплой уязвимых сервисов и лабораторий
- Vagrant: Скриптуемое окружение
- Kali / Parrot OS / BlackArch: Специализированные дистрибутивы