* **01 – Information Gathering (Сбор информации)**
* DNS Analysis (анализ DNS)
* IDS/IPS Identification (идентификация IDS/IPS, файерволов)
* Live Host Identification (идентификация хостов)
* Network and Port Scanners (сканеры сети и портов)
* OSINT Analysis (разведка на основе открытых источников)
* Route Analysis (анализ маршрутов)
* SMB Analysis (анализ SMB)
* SMTP Analysis (анализ SMTP)
* SNMP Analysis (анализ SNMP)
* SSL Analysis (анализ SSL)
* **02 – Vulnerability Analysis (Анализ уязвимостей)**
* Cisco Tools (инструменты Cisco)
* Fuzzing Tools (инструменты фаззинга)
* OpenVAS Scanner
* Stress Testing (стресс-тестирование)
* VoIP Tools (инструменты VoIP)
* **03 –Web Application Analysis (Анализ веб-приложений)**
* CMS and Site Identification (идентификация систем управления контентом и сайтов)
* WebApp Proxies (веб-прокси)
* Web Crawlers & Directory Brut-forcers (веб-обходчики и брут-форсеры директорий и файлов)
* Web Vulnerability Scanners (сканеры веб-уязвимостей)
* **04 – Database Assessment (Оценка баз данных)**
* **05 – Password Attacks (Атаки на пароли)**
* Offline Attacks (офлайн атаки)
* Online Attacks (онлайн атаки)
* Passing the Hash tools
* Password Profiling & Wordlists (профилирование паролей и словари)
* **06 – Wireless Attacks (Беспроводные атаки)**
* 802.11 Wireless Analysis (анализ Wi-Fi)
* Bluetooth Tools (инструменты Bluetooth)
* Other Wireless Tools (другие беспроводные инструменты)
* RFID & NFC Tools (инструменты RFID и NFC)
* Software Defined Radio (программно-определяемая радиосистема)
* **07 – Reverse Engineering (Обратная инженерия)**
* **08 – Exploitation Tools (Инструменты эксплуатации)**
* **09 – Sniffing & Spoofing (Сниффинг и спуфинг)**
* Network Sniffers (сетевые снифферы)
* Spoofing and MITM (спуфинг и атака человек-посередине)
* **10 – Post Exploitation (Последующая эксплуатация, поддержка доступа)**
* OS Backdoors (бэкдоры операционных систем)
* Tunneling & Exfiltration (туннелирование и эксфильтрация)
* Web Backdoors (бэкдоры веб-сайтов)
* **11 – Forensic (IT криминалистика)**
* Digital Forensics (цифровая криминалистика)
* Forensic Carving Tools (криминалистическое выскабливание данных)
* Forensic Imaging Tools (работа с образами медиа носителей)
* PDF Forensics Tools (криминалистические инструменты работы с PDF)
* Sleuth Kit Suite (набор инструментов Sleuth Kit)
* **12 – Reporting Tools (Инструменты составления отчётов)**
* **13 – Social Engineering Tools (Инструменты для социальной инженерии)**
* **14 – System Services (Системные службы)**
* BEEF XSS Framework
* Dradis
* OpenVas
* Xplico

Два молодых ресурса, нацеленные главным образом на практику, в настоящее время активно пополняются актуальным материалом:

* [https://kali.tools](https://kali.tools/)
* [https://hackware.ru](https://hackware.ru/)