Hacking & Penetesting Tools

Information Gathering
- DNS Analysis: dnsenum, dnsrecon, fierce
- IDS/IPS Identification: lbd, wafw00f
- Live Host Identification: arping, fping, hping3, thcping6, masscan
- Network & Port Scanners: masscan, nmap
- OSINT Analysis: spiderfoot, spiderfoot-cli, thehravester
- Route Analysis: netdiscover, netmask
- SMB Analysis: enum4linux, smbmap, nbtscan
- SMTP Analysis: swaks
- SNMP Analysis: snmp-check, onesixtyone
- SSL Analysis: sssldump, sslh, sslyze, sslcan

Vulnerability Analysis
- Fuzzing Tools: spike-generic_chunked, spike-generic_listen_tcp, spike-generic_send_tcp, spike-generic_send_udp
- VoIP Tools: voiphopper

Web Application Analysis
- CMS & Framework Identification: wpscan
- Web Application Proxies: burpsuite
- Web Crawlers & Directory Bruteforce: cutycapt, dirb, ffuf, dirbuster, wfuzz
- Web Vulnerability Scanners: cadaver, davtest, nikto, skipfish, wapiti, whatweb, wpscan

Database Assessment
- SQLite database browser
- sqlmap

Password Attacks
- Offline Attacks: chntpw, hashcat, hashid, hash-identifier, ophcarck-cli, samdump2
- Online Attacks: onesixtyone, hydra, patator, thc-pptp-bruter
- Passing the Hash Tools: mimikatz, smbmap, pth-curl, pth-net, pth-winexe
- Password Profiling & Wordlists: crunch, cewl, rsmangler, wordlists

Wireless Attacks
- 802.11 Wireless Tools: bully, fern wifi cracker(root)
- Bluetooth Tools: spooftooph

Reverse Engineering
- clang, clang++, NASM shell, radare2

Exploitation Tools
- crackmapexec, metasploit framework, msf-payload creator, searchsploit, social engineering toolkit (root), sqlmap

Sniffing & Spoofing
- Network Sniffers: dnschef, netsniff-ng, wireshark
- Spoofing & MITM: etercap, dnschef, rebind, sslsplit, tcpreplay

Post Exploitation
- OS Backdoors: dbd, powersploit, sbd
- Tunneling & Exfiltration: dns2tcpc, exe2hex, dns2tcpd, exe2hex, iodine, miredo, proxychains4, proxytunnel, ptunnel, pwnat, sslh, stunnel4, udptunnel
- Web Backdoors: laudanum, weevely

Forensics
- Forensic Carving Tools: magisrescue, scalpel, scrounge-ntfs
- Forensic Imaging Tools: guymager (root), pdfid, pdf-parser
- Sleuth Kit Suite: autopsy(root), blkcalc, blkcat, blkls, blkstat, ffind, fsstat, fls, hfind, icat-sleuthkit, ifind, ils-sleuthkit, img_cat, istat, jls, jcat, mactime-sleuthkit, mmcat, mmls, mmstat, sigfind, sorter, srch_strings, tsk_comparedir, tsk_gettimes, tsk_recover, tsk_loaddb

Reporting Tools
- cutycapt, faradday start, pipal, recordmydesktop

Social Engineering Tools
- msf payload creator, social engineering toolkit (root)